



INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Trabajo Terminal II.

Autentificación mediante Chaffing and Winnowing en el protocolo HTTP

2018-B003.

Integrantes:

Blancas Pérez Bryan Israel
Carrillo Fernández Gerardo
Morales González Diego Arturo
Paredes Hernández Pedro Antonio

Directores:

Moreno Cervantes Axel Ernesto
Díaz Santiago Sandra

Índice.

1. Introducción	8
1.1. Objetivos	9
1.1.1. Objetivo general	9
1.1.2. Objetivos particulares	9
1.2. Trabajo previo	10
1.2.1. Kerberos (CISCO)	10
1.2.2. Tririga (IBM)	11
1.3. Justificación	12
1.4. Metodología	13
1.5. Organización del documento	16
1.5.1. Capítulo 2. Marco teórico.	16
1.5.2. Capítulo 3. Análisis.	16
1.5.3. Capítulo 4. Diseño.	16
1.5.4. Capítulo 5. Desarrollo.	16
1.5.5. Capítulo 6. Avances y trabajo por hacer.	17
2. Marco teórico	18
2.1. Protocolo HTTP	18
2.1.1. Solicitud HTTP	19
2.1.2. Respuesta HTTP	19
2.2. Certificado	20
2.3. Métodos de autentificación en internet.	21
2.4. Cookies.	24
2.5. Introducción a la Criptografía.	26
2.5.1. Criptología.	26
2.5.2. Criptografía.	27
2.5.3. Objetivos de la criptografía.	28
2.5.4. Usos de la criptografía.	29
2.5.5. Criptografía simétrica y asimétrica.	29
2.5.6. Criptografía a nivel de aplicación.	33
2.6. Chaffing and Winnowing.	34

2.6.1.	Historia	34
2.6.2.	¿Qué es Chaffing and Winnowing?	34
2.6.3.	Objetivo de Chaffing and Winnowing	36
2.6.4.	¿Cómo funciona?	37
2.6.5.	Propiedades de Chaffing and Winnowing	39
2.6.6.	All-or-Nothing and the Package Transform (AONT) .	39
2.6.7.	Comparando Chaffing and Winnowing contra Cifrado y Esteganografía	42
3. Análisis.		45
3.1.	Estudio de Factibilidad.	45
3.1.1.	Factibilidad Técnica	45
3.1.2.	Factibilidad Operativa	47
3.1.3.	Factibilidad Económica	48
3.2.	Herramientas a usar.	49
3.2.1.	Software.	49
3.2.2.	Hardware.	53
3.3.	Arquitectura del sistema.	54
3.3.1.	Descripción de la arquitectura del sistema.	55
3.4.	Diagrama de casos de uso general.	56
3.5.	Componente I. Extensión.	56
3.5.1.	Descripción.	56
3.5.2.	Estudio de requerimientos.	57
3.5.3.	Reglas del negocio.	59
3.6.	Componente II: Servidor autentificador.	60
3.6.1.	Descripción.	60
3.6.2.	Estudio de requerimientos.	61
3.6.3.	Reglas del negocio.	62
3.7.	Componente III: Servicio Web y API.	62
3.7.1.	Descripción.	62
3.7.2.	Estudio de requerimientos.	63
4. Diseño.		65
4.1.	Componente I.	65
4.1.1.	Diagrama de casos de uso	65
4.1.2.	Descripción de casos de uso.	66
4.1.3.	Diagrama de flujo (DF).	79
4.1.4.	Diagrama de flujo de datos (DFD).	81
4.1.5.	Diagrama de clases.	83
4.1.6.	Diagramas de secuencia.	88
4.1.7.	Diagrama de actividades	97

4.1.8. Interfaz de usuario.	98
4.1.9. Requisitos de diseño.	100
4.1.10. Algoritmos.	102
5. Desarrollo	106
5.1. Componente I.	106
6. Avances y trabajo por hacer.	111

Índice de figuras.

1.1. Fases de la metodología por prototipos	14
2.1. Comunicación Cliente - Servidor en el protocolo HTTP	18
2.2. Firma de un certificado por una AC.	21
2.3. Verificación de un certificado firmado por una AC.	21
2.4. Esquema del protocolo de criptografía simétrica.	30
2.5. Esquema del protocolo de criptografía asimétrica.	31
2.6. Charles agrega los paquetes inválidos.	35
2.7. Charles no agrega los paquetes pero multiplexa los flujos.	36
2.8. Secuencia de Chaffing después del proceso de autentificación. .	38
2.9. Formas del proceso de chaff	38
2.10. Visión general del proceso Chaffing and Winnowing.	39
2.11. Proceso de Chaffing and Winnowing junto con AONT.	41
3.1. Arquitectura General del Sistema	54
3.2. Diagrama de casos de uso general del sistema	56
4.1. Diagrama de casos de uso del Componente I.	65
4.2. Diagrama de flujo del Componente I.	79
4.3. Diagrama de flujo de datos del Componente I.	81
4.4. Diagrama de clases de Componente I.	83
4.5. Diagrama de secuencia 1 del Componente I	88
4.6. Diagrama de secuencia 2 del Componente I	89
4.7. Diagrama de secuencia 3 del Componente I	90
4.8. Diagrama de secuencia 4 del Componente I	91
4.9. Diagrama de secuencia 5 del Componente I	92
4.10. Diagrama de secuencia 6 del Componente I	93
4.11. Diagrama de secuencia 7 del Componente I	94
4.12. Diagrama de secuencia 8 del Componente I	95
4.13. Diagrama de secuencia 9 del Componente I	96
4.14. Diagrama de actividades del Prototipo 2.	97
4.15. Pantalla inicial.	98

4.16. Tab de la extensión. Permite inicio de sesión	99
4.17. Mensaje de éxito	99
4.18. Mensaje de error	100
4.19. Mensaje de error en certificado	100
4.20. Arreglo del patrón de chaffing	104
4.21. Arreglo del patrón de chaffing después de una iteración	104
4.22. Arreglo del patrón de chaffing final	104
4.23. Arreglo chaff final.	105
5.1. Inicio de sesión para la obtención del certificado.	106
5.2. Aviso de guardado del certificado en Storage.	107
5.3. Pagina bloqueada del lado del cliente.	108
5.4. Wireshark analizando en red WI-FI filtrando análisis por <i>http</i>	109
5.5. Análisis de petición en <i>Show Packet Bytes</i>	110

Índice de cuadros.

1.1.	Tabla comparativa de estado del arte	12
2.1.	Aplicación de los métodos de autentificación	22
2.2.	Seguridad en los métodos de autentificación	23
3.1.	Herramientas de Software	46
3.2.	Equipo de Hardware 1	46
3.3.	Equipo de Hardware 2	46
3.4.	Equipo de Hardware 3	47
3.5.	Horas de trabajo	48
4.1.	DCU: CI_CU1	66
4.2.	DCU: CI_CU2	67
4.3.	DCU: CI_CU3	68
4.4.	DCU: CI_CU4	69
4.5.	DCU: CI_CU5	70
4.6.	DCU: CI_CU6	72
4.7.	DCU: CI_CU7	73
4.8.	DCU: CI_CU8	75
4.9.	DCU: CI_CU9	77

Glosario.

Cookies Es una pequeña información enviada por un sitio web y almacenada en el navegador del usuario, de manera que el sitio web puede consultar la actividad previa del navegador. Sus principales funciones son recordar accesos y conocer información sobre los hábitos de navegación e intentos de spyware. 24

Flash Aplicación informática englobada en la categoría de reproductor multimedia. 50

HTTP Hypertext Transfer Protocol. 57, 66

ID identificador. 22

Identity theft También conocido como "robo de identidad" se produce cuando una persona adquiere, transfiere, posee o utiliza información personal de una persona física o jurídica de forma no autorizada, con la intención de efectuar o vincularlo con algún fraude u otro delito. 24

IU Interfaz de Usuario. 59

Netcape Navegador web de la compañía NetScape Communications. 51

Single Sign-On Es un procedimiento de autenticación que le permite a un usuario determinado acceder a varios sistemas con una sola instancia de identificación.. 11

Capítulo 1

Introducción

En la actualidad la mayoría de los usuarios de internet necesitan guardar contraseñas para sus distintas cuentas en las diferentes páginas web a las que ingresan, ya que recordarlas es un problema debido a la gran cantidad de servicios que se utilizan. Como consecuencia de que la autentificación por contraseña es la más utilizada en los servicio web hoy en día [15], estos han implementado mecanismos de seguridad tales como contraseñas que contengan un mínimo de caracteres determinados, al menos un carácter especial, considerar no incluir datos fáciles como nombres, fechas de nacimiento, entre otros. Como consecuencia, éstas son más difíciles de recordar y han orillado a los usuarios a optar por guardarlas en medios físicos o digitales para recordarlas cuando sea necesario. Sin embargo, perder esas claves presenta un grave problema de seguridad, teniendo como consecuencia: perdida de datos sensibles, robo de identidad, robo de cuentas bancarias, etc [7].

La gran mayoría de servicios web han implementado la función "recordar contraseña", la cual hace que el usuario no tenga que ingresar sus credenciales¹ cada vez que se quiere acceder al servicio.

El método *Chaffing and Winnowing* proporciona confidencialidad de los mensajes sin la necesidad de usar métodos de cifrado o esteganografía[3], agregando 'basura' (*Chaffing*) para que el mensaje quede ininteligible ante la vista de terceros no implicados en la comunicación, y sólo el receptor pueda 'limpiar' (*Winnowing*) el mensaje obteniendo la información relevante.

Es por ello que en este trabajo terminal se propone realizar un nuevo método de autentificación por medio del método de *Chaffing and Winnowing* con la ayuda de una extensión de Google Chrome, la cual servirá para la

¹Credenciales se entiende como los datos que un servicio web requiere para poder acceder a él. Comúnmente son 'usuario' y 'contraseña'.

inyección del certificado de autentificación en el protocolo HTTP, emitido por un servidor autenticador que proveerá al usuario un certificado, utilizando una autoridad certificadora basándose en los datos del mismo (Usuario y Contraseña). El usuario obtendrá este certificado al iniciar sesión una única vez en la extensión, y una vez teniendo este certificado, solo será necesario iniciar sesión una vez en cada servicio, ya que el certificado se asociará a esta cuenta y posteriormente cuando el usuario quiera acceder, se validará este certificado para dar respuesta al usuario. Así, si un servicio web tiene este tipo de autentificación disponible, lo podrá validar. Esto es, poder hacer el proceso de *Winnowing* con el cual podrá obtener el certificado original y poder validarla. El propósito principal de este trabajo es que los usuarios puedan realizar un inicio de sesión más cómodo, seguro y sin la necesidad de recordar sus distintas contraseñas constantemente.

1.1. Objetivos.

1.1.1. Objetivo general.

Realizar un nuevo método de autentificación modificando los datos de la cabecera del protocolo HTTP utilizando Chaffing and Winnowing con la ayuda de una extensión del navegador Google Chrome.

1.1.2. Objetivos particulares.

- Investigar e implementar el desarrollo de extensiones en Google Chrome.
- Investigar sobre los mecanismos de autentificación.
- Investigar sobre la técnica de *Chaffing and Winnowing* para adaptar su implementación.
- Inyectar el certificado autenticador (*Chaffing*) en el encabezado HTTP para enviar la petición al servidor.
- Implementación de un Login en la extensión de Google Chrome.
- Investigar sobre Autoridades Certificadoras para implementar un servidor autenticador
- Generación de certificado autenticador del usuario
- Implementación de un servicio web de prueba.

- Desarrollo de un API para nuestro servidor que obtenga el certificado del usuario (*Winnowing*).
- Modificar el código del servidor Apache para simular y comprobar el funcionamiento de la extensión.
- Realizar pruebas de seguridad para comprobar la eficacia de la extensión.

1.2. Trabajo previo.

Con la finalidad de darle al lector un panorama más amplio sobre la importancia y el impacto del trabajo terminal a desarrollar, se procede a explicar otros servicios similares al que se presenta en este trabajo:

1.2.1. Kerberos (CISCO)

Kerberos es un servicio confiable de autenticación de terceros basado en el modelo presentado por Needham y Schroeder. Cuando un usuario hace peticiones a un servicio, su identidad debe ser establecida. Para hacer esto, un boleto² se presenta al servidor, junto con la prueba que el boleto fue publicado al usuario, y no fue robado originalmente.

Kerberos guarda en una base de datos sus clientes y sus claves privadas. La clave privada es un número grande que solamente conoce Kerberos y el cliente y la cual esta cifrada. Los servicios de red que requieren la autenticación se registran en Kerberos, al igual que los clientes que desean utilizar esos servicios.

Kerberos también genera las claves privadas temporales, llamadas las claves de la sesión, que se dan a dos clientes y nadie más. Una clave de la sesión se puede utilizar para cifrar los mensajes entre estos.

Cada mensaje no sólo se autentica si no también se cifra. Los mensajes privados son utilizados, por ejemplo, por el servidor de Kerberos para enviar las contraseñas sobre la red [28].

²Un boleto contiene el nombre del servidor, el nombre del cliente, la dirección de Internet del cliente, un grupo fecha/hora, un curso de la vida, y una clave de sesión aleatoria. Se utiliza para pasar con seguridad la identidad de la persona a quien le fue publicado el boleto entre el servidor de autenticación y el servidor externo.

1.2.2. Tririga (IBM)

IBM ha implementado una autenticación de usuarios mediante el inicio de sesión único, la ultima versión (IBM Tririga Application Platform 3.6.0) fue creada en el año 2018 [12]. Esta autenticación está implementada para obtener acceso a **IBM Tririga**³, en esta plataforma es necesario autenticar un usuario como usuario valido del sistema y concederle acceso a las aplicaciones y funciones de la suite⁴ de aplicaciones de IBM Tririga. El inicio de sesión único (Single Sign-On) proporciona a los usuarios una vía para gestionar el acceso a varias aplicaciones de su entorno [13].

Tririga Application Platform utiliza su propia autenticación nativa de forma predeterminada. Con la autenticación nativa, el usuario especifica su nombre de usuario y su contraseña en una pantalla de inicio de sesión de IBM Tririga, luego entonces, la plataforma autentifica el usuario comparando el nombre de usuario y la contraseña almacenados en la base de datos de IBM Tririga [13].

El proceso de este tipo de autenticación de Tririga es el siguiente:

- El usuario especifica la URL del servidor web en un navegador o accede a la aplicación mediante un cliente.
- Es posible que se le solicite al usuario que especifique un nombre de usuario o una contraseña, o bien que se inicie la sesión inmediatamente. El inicio de sesión inmediato, sin que el servidor cuestione al navegador o al cliente, no está soportado en algunas configuraciones.
- El servidor web, el servidor de aplicaciones o el plug-in de autenticación verifica la información con el origen de la autenticación.
- Si el inicio de sesión es satisfactorio, el servidor web añade las credenciales de usuario a la cabecera HTTP y las envía al servidor de aplicaciones.
- El servidor de aplicaciones procesa las credenciales de usuario e inicia la sesión en la aplicación.

³IBM Tririga es un sistema de gestión del espacio de trabajo integrado (IWMS) que incrementa el rendimiento operativo, financiero y medioambiental de sus instalaciones y bienes inmuebles.

⁴El término suite hace referencia a un conjunto de aplicaciones y herramientas de software incluidas en un sólo paquete y que, por lo general, comparten un aspecto similar y se integran entre sí.

	Ventajas	Desventajas
Kerberos	<ul style="list-style-type: none"> - Kerberos proporciona una interfaz para los clientes de la aplicación y los servidores de aplicaciones. - Métodos de cifrado seguros y rápidos. - Aislamiento de información sensible y no sensible. - Es posible tener copias de la base de datos en diversas máquinas auxiliares. 	<ul style="list-style-type: none"> - El curso de vida de un boleto debe tener un balance adecuado entre seguridad y conveniencia. - La información puede ser vulnerada si el usuario olvida finalizar su sesión. - Posibles problemas de compatibilidad con las proxys.
Tririga	<ul style="list-style-type: none"> - Soporta los métodos de inserción del nombre de usuario en una cabecera HTTP. - Distinción entre mayúsculas y minúsculas. - Eliminación de nombre de dominio. 	<ul style="list-style-type: none"> - Se puede crear una vulnerabilidad al mantener abierto el puerto HTTP. - Este servicio es exclusivo para un usuario en específico.

Cuadro 1.1: Tabla comparativa de los diferentes servicios

Es por esto que se propone una nueva alternativa de autenticación que brinda al usuario el acceso a cada uno de sus servicios web. El usuario se autenticará una sola vez en cada servicio, sin la necesidad de almacenar sus datos sensibles ⁵ en medios ajenos al servicio.

1.3. Justificación.

Nuestro trabajo busca autenticar a los usuarios en los distintos servicios web de su preferencia, utilizando *Chaffing and Winnowing*, debido a que nos brinda confidencialidad a un menor costo computacional [3]. Además, buscamos quitarle al usuario la necesidad de iniciar sesión continuamente en un servicio web, ya que, en este nuevo método de autenticación propuesto, el usuario sólo debe ingresar una única vez al servicio web que desea usar.

Por medio un servidor autenticador, obtendremos un certificado real para

⁵Un dato sensible es un dato que requiere una mayor protección que el resto de datos de carácter personal.

cada usuario con el que se autentificará. Gracias a que el servidor autenticador es externo a la extensión y al servicio web, el usuario podrá acceder a sus cuentas sin importar que sean computadoras diferentes, siempre y cuando tengan instalada la extensión.

1.4. Metodología.

El proceso de desarrollo que seguiremos estará basado en la metodología de **"Prototipos Evolutivos"** con unas pequeñas adaptaciones que realizamos para que pueda funcionar mejor en el proceso de realización del sistema. Esta metodología ayuda a los desarrolladores a mejorar la comprensión del trabajo terminal a elaborar cuando los requerimientos no están completamente definidos o pueden ir cambiando a lo largo de la implementación . Así mismo, el paradigma nos brinda la posibilidad de utilizar fragmentos de programas existentes o aplicar herramientas que nos permitan generar rápidamente proyectos que funcione y puedan evolucionar [22].

Al utilizar este paradigma de desarrollo se busca que, mediante la implementación parcial del trabajo, vayan surgiendo requerimientos no vistos desde el planteamiento del problema, de esta manera, nos es posible ir experimentando con un prototipo parcialmente funcional e identificar posibles mejoras o fallas, con el fin de lograr el objetivo final.

En la Figura 1.1, se muestra un diagrama de las fases de esta metodología. Primeramente, tenemos la fase de 'Comunicación' en donde el equipo de desarrollo se reúne para definir los objetivos generales del trabajo terminal, se identifican los requerimientos conocidos y se detectan las áreas de mayor atención. Después, se llevan a cabo las fases 'Plan rápido' y 'Diseño rápido' en donde se hace un análisis del prototipo actual y se modela para dar paso al desarrollo del prototipo ('Construcción del prototipo'). Finalmente, para terminar una iteración, se realiza la fase 'Despliegue, entrega y retroalimentación' en donde se evalúa el funcionamiento realizando pruebas que nos brindan una retroalimentación para mejorar los requerimientos [22].

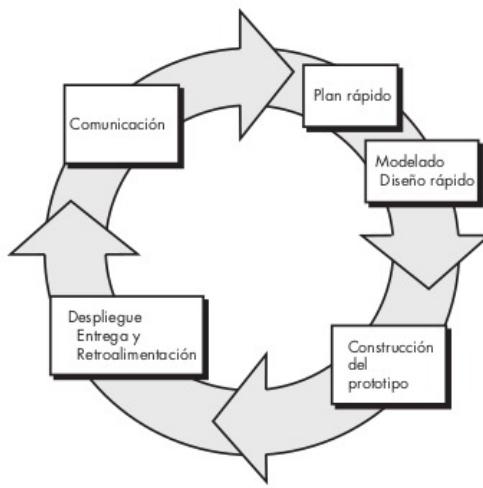


Figura 1.1: Diagrama de los fases de la metodología de prototipos evolutivos.

Para nuestro trabajo terminal y como primera fase vamos a realizar un prototipo con el fin de evaluarlo y considerar mejoras para la siguiente evolución del mismo. No se conoce el número total de prototipos que se deban realizar y para evaluarlos será necesario implementar cada uno de estos, es importante resaltar que nuestro sistema se encuentra conformado por componentes y que en algunos casos existe dependencia por lo que es indispensable considerar que para el correcto funcionamiento del prototipo se debe realizar un componente mucho antes que otro.

A continuación se indica cada una de las etapas de la metodología con lo que se realizará en cada una de estas:

1. Comunicación y plan rápido
 - Reunir requerimientos del prototipo
 - Componente 1
 - Investigar sobre el desarrollo de extensiones en Google Chrome.
 - Investigar sobre el método Chaffing and Winnowing.
 - Componente 2
 - Investigar sobre Certificados
 - Investigar sobre Autoridades Certificadoras.
 - Componente 3
 - Investigación sobre el servidor Apache.

- Analizar la arquitectura del servidor Apache
- Investigación sobre la versión de Apache conveniente a modificar.
- Describir el prototipo.

2. Modelado y diseño rápido

- Componente 1
 - Modelar un algoritmo que genere un patrón de chaffing.
 - Modelar un algoritmo de chaffing.
 - Crear un método que reciba un certificado, una cabecera HTTP y el patrón.
 - Diseñar una cabecera HTTP modificada que pueda contener la información de autenticación
- Componente 2
 - Diseñar una Base de datos para almacenar los datos del usuario y su certificado.
- Componente 3
 - Diseñar una API en el servicio web que permita interceptar una petición HTTP.
 - Diseñar una arquitectura del sistema.

3. Construcción del prototipo

- Componente 1
 - Implementar el algoritmo de chaffing.
 - Implementar una extensión que intercepte peticiones HTTP.
 - Implementar un login en donde el usuario pueda iniciar sesión.
- Componente 2
 - Implementar la Autoridad Certificadora.
 - Implementar un Servidor que reciba y envíe peticiones.
- Componente 3
 - Implementar un servidor Apache.
 - Implementar una API que reciba una petición y pueda identificarla.

4. Despliegue, entrega y Retroalimentación:

Después de la implementación del prototipo se analizará si puede haber mejoras y si es conveniente la realización de otro prototipo evolucionando este o desechándolo.

1.5. Organización del documento

Para dar inicio a este trabajo terminal, presentamos de manera breve la estructura de este reporte, con el objetivo de que el lector pueda tener un mejor entendimiento del trabajo.

1.5.1. Capítulo 2. Marco teórico.

Dado que este trabajo terminal relaciona temáticas muy enfocadas a la seguridad y aspectos web, es necesario conocer algunos conceptos e ideas fundamentales tanto para entenderlo como para conocer su funcionamiento, por lo tanto será necesario hablar del protocolo HTTP, métodos de autenticación, criptografía y acerca del método *Chaffing and Winnowing* que es la parte medular de todo este trabajo; en este marco teórico se explicará de manera breve y con un enfoque directo el uso que le daremos a estos conceptos en el trabajo terminal.

1.5.2. Capítulo 3. Análisis.

Dentro de este capítulo se analiza el estudio de factibilidad tanto técnico como operativo y económico con la finalidad de conocer los recursos necesarios para la elaboración de este trabajo terminal. Se mencionan de manera resumida las herramientas a utilizar y se explica de manera general la arquitectura del sistema y el diagrama de casos de uso general. Finalmente se muestra el análisis de los 3 componentes que tenemos en el sistema.

1.5.3. Capítulo 4. Diseño.

En el tercer capítulo, no adentraremos en el desarrollo de los prototipos, es decir, se encuentran los diagramas pertinentes para poder modelar nuestro trabajo terminal y proceder a la etapa de codificación. En este capítulo se desarrollan y explican los siguientes diagramas: 'Casos de uso', 'Flujo', 'Flujo de datos', 'Clases', 'Secuencia' y 'Actividades' y se muestra la interfaz de usuario propuesta junto con los requisitos de diseño.

1.5.4. Capítulo 5. Desarrollo.

En este capítulo, mostraremos lo que hemos desarrollado para este TT1 (Componente I). Se muestra que el prototipo cumpla los requerimientos que se le impusieron en la sección de análisis.

1.5.5. Capítulo 6. Avances y trabajo por hacer.

En el último capítulo de este reporte, hablaremos de los avances que hemos logrado a lo largo de la asignatura de trabajo terminal I y además, exponemos el trabajo esperado para la asignatura de trabajo terminal II.

Capítulo 2

Marco teórico

2.1. Protocolo HTTP

Desde 1990, el protocolo HTTP (Hypertext Transfer Protocol, Protocolo de transferencia de hipertexto) es el protocolo más utilizado en Internet. La versión 0.9 solo tenía la finalidad de transferir los datos a través de Internet (en particular páginas web escritas en HTML). La versión 1.0 del protocolo (la más utilizada) permite la transferencia de mensajes con encabezados que describen el contenido de los mensajes mediante la codificación MIME.

El propósito del protocolo HTTP es permitir la transferencia de archivos (principalmente, en formato HTML), entre un navegador (el cliente) y un servidor web (denominado, entre otros, httpd en equipos UNIX) localizado mediante una cadena de caracteres denominada dirección URL.

La comunicación entre el navegador y el servidor al que se quiere acceder se realiza de la siguiente manera en la figura 2.1:

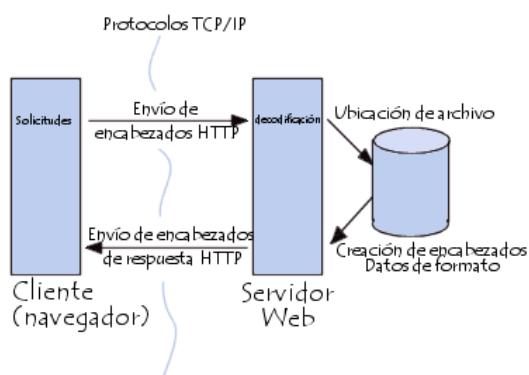


Figura 2.1: Comunicación Cliente - Servidor en el protocolo HTTP

El navegador realiza una solicitud HTTP y el servidor procesa la solicitud y después envía una respuesta HTTP. En realidad, la comunicación se realiza en más etapas si se considera el procesamiento de la solicitud en el servidor. Dado que sólo nos ocupamos del protocolo HTTP, no se explicará la parte del procesamiento en el servidor en esta sección del artículo[5].

2.1.1. Solicitud HTTP

Una solicitud HTTP es un conjunto de líneas que el navegador envía al servidor. Comprende:

- **Una línea de solicitud:** una línea que especifica el tipo de documento solicitado, el método que se aplicará y la versión del protocolo utilizada. La línea está formada por tres elementos que deben estar separados por un espacio: el método, la dirección URL y la versión del protocolo utilizada por el cliente (por lo general, HTTP/1.0)
- **Los campos del encabezado de solicitud:** un conjunto de líneas opcionales que permiten aportar información adicional sobre la solicitud y/o el cliente (navegador, sistema operativo, etc.). Cada una de estas líneas está formada por un nombre que describe el tipo de encabezado, seguido de dos puntos (:) y el valor del encabezado.
- **El cuerpo de la solicitud:** un conjunto de líneas opcionales que deben estar separadas de las líneas precedentes por una línea en blanco y, por ejemplo, permiten que se envíen datos por un comando POST durante la transmisión de datos al servidor utilizando un formulario.

2.1.2. Respuesta HTTP

Una respuesta HTTP es un conjunto de líneas que el servidor envía al navegador. Está constituida por:

- **Una línea de estado:** una línea que especifica la versión del protocolo utilizada y el estado de la solicitud en proceso mediante un texto explicativo y un código. La línea está compuesta por tres elementos que deben estar separados por un espacio: la versión del protocolo utilizada, el código de estado y el significado del código.
- **Los campos del encabezado de respuesta:** un conjunto de líneas opcionales que permiten aportar información adicional sobre la respuesta y/o el servidor. Cada una de estas líneas está compuesta por un

nombre que califica el tipo de encabezado, seguido por dos puntos (:) y por el valor del encabezado.

- **El cuerpo de la respuesta:** contiene el documento solicitado.

2.2. Certificado

Un certificado digital (X.509, v.3) es un fichero que contiene (entre otros datos) la clave pública (y privada) de una persona y está avalado (firmado electrónicamente) por una entidad de confianza o *Autoridad de Certificación*.

La Fabrica Nacional de Moneda y Timbre (FNMT) emite certificados digitales (los certificados del Documento Nacional de Identidad [DNI] están emitidos por la Dirección General de la Policía - Fabrica Nacional de Moneda y Timbre [DGP-FNMT]) [30].

El certificado digital contiene, entre otros datos, los siguientes:

- Filiación del propietario (Nombre, DNI, email).
- Protocolo de firma que se lleva a cabo (C,D).
- Autoridad de certificación que emite el certificado (FNMT).
- Fecha de emisión y de caducidad (2-3 años).
- Clave publica -privada- del propietario ($K -k-$).
- Firma electrónica de la autoridad de certificación.

Todo certificado debe estar firmado electrónicamente por una Autoridad de Certificación (AC) para ser valido. Este proceso de firma lo lleva a cabo la AC a la vez que genera el certificado (Figura 2.2), se lleva a cabo de la siguiente manera:

- Recopila los datos del usuario y las claves generadas por su navegador.
- Calcula un resumen (hash) de todos los datos recopilados. Firma electrónicamente el resumen anterior y lo une a los datos recopilados (Valor de la firma del certificado o Huella digital).

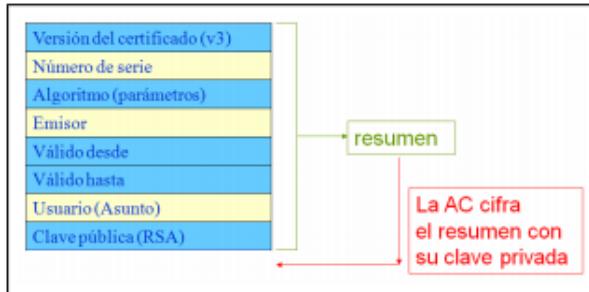


Figura 2.2: Firma de un certificado por una AC.

Antes de que un certificado personal (el único que puede tener claves privadas) sea instalado en el almácen de un navegador, éste verifica que está firmado por una AC (Figura 2.3) de las incluidas en su almácen de certificados (Autoridades) de la siguiente manera:

- Calcula el resumen (hash) de todos los datos recopilados del certificado, sin incluir la firma electrónica de la Autoridad Certificadora.
- Descifra la firma del certificado con la clave pública de la AC (debe estar en su almácen de Autoridades).
- Compara el resumen calculado con lo descifrado y decide sobre su autenticidad.

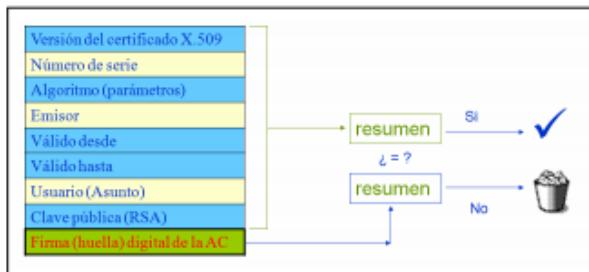


Figura 2.3: Verificación de un certificado firmado por una AC.

2.3. Métodos de autentificación en internet.

Con la evolución de la web, distintas páginas ofrecen ciertos servicios a los usuarios y con la finalidad de dar una experiencia óptima y segura, se

requiere que una persona o usuario se identifique para el uso de estos servicios, es aquí donde entra en juego el papel de los métodos de autenticación. Para poder asegurar la confidencialidad de la información manejada en todos estos servicios, es necesario restringir el acceso de este, para esto se utiliza la identificación y la autenticación; la identificación es un procedimiento donde el sujeto es reconocido por algún ID, esto es equivalente al saber una parte de información en específico, mientras que la autenticación es el proceso de validación de si el sujeto es la persona quien dice ser al tratar de identificarse [15].

Para probar una identidad, el sujeto presenta algo llamado "factor de autenticación", principalmente existen 4:

- El sujeto tiene algo (Token, documento, un material específico, etc.).
- El sujeto conoce algo (contraseña, login, respuesta a una pregunta, etc.).
- El sujeto tiene una característica biológica (huella dactilar, ADN, etc.).
- El sujeto se encuentra en un lugar en específico (dirección IP, información de un lugar en específico, etc.).

Hoy en día, la autenticación por contraseña es el método más utilizado, más que otra cosa por su ventaja principal: su simplicidad de utilización, sin embargo, así como tiene una gran ventaja, la autenticación por contraseña también tiene muchos problemas y desventajas de seguridad.

A continuación en el cuadro 2.1, mostraremos algunas tablas comparativas que servirán para tener una mejor perspectiva de las ventajas, desventajas, vulnerabilidades de los diferentes métodos de autenticación, entre otras cosas:

	Recordar	Otros dispositivos	Acciones	Facilidad	Tiempo	Errores	Recuperación
Contraseñas	1	3	2	3	3	2	3
Otros recursos	2	3	3	3	3	3	2
Contraseñas gráficas	1	1	2	3	3	2	3
Contraseñas dinámicas	1	3	2	2	3	2	2
Tokens	3	1	1	2	2	3	1
Multivariación	1	1	1	3	2	2	1
Cryptograffía	3	1	1	1	1	2	1
Biométricos	3	3	2	3	2	2	1

Cuadro 2.1: Tabla comparativa de la aplicación en los distintos métodos de autenticación

La tabla anterior concentra las siguientes características:

- Recordar: Hace referencia a que tan complicado es que un usuario se acuerde de los datos necesarios para la autentificación.
- Otros dispositivos: El usuario usa una entidad externa para facilitar su autentificación.
- Acciones: Hace referencia a que tantas acciones adicionales se deben de realizar para autentificarse.
- Facilidad: Simplicidad de tecnología.
- Tiempo: Cantidad de recursos temporales que consume el método de autentificación.
- Errores: Posibles errores durante la autentificación.
- Recuperación: Denota la dificultad de recuperar la clave de acceso en caso de pérdida.

En el cuadro 2.2 se muestra una tabla comparativa del nivel de seguridad en los distintos métodos de autentificación, donde 1 - baja seguridad, 2 – media seguridad y 3 – alta seguridad.

	Ataque por fuerza bruta	Observación	Hackeo indirecto	Phishing
Contraseñas	1	1	1	1
Otros recursos	2	2	3	3
Contraseñas gráficas	1	1	2	2
Contraseñas dinámicas	2	3	2	2
Tokens	3	3	3	3
Multivariación	1	1	3	3
Criptografía	3	3	3	3
Biométricos	3	3	1	1

Cuadro 2.2: Tabla comparativa de la seguridad en los distintos métodos de autentificación

La tabla se enfoca principalmente en los siguientes problemas de seguridad:

- Ataque por fuerza bruta: Se descifra el método de autentificación con una gran cantidad de intentos, usualmente generados por un programa.

- Observación: Cuando se intenta ver directamente los datos necesarios para la autentificación desde una distancia cercana hasta incluso usando binoculares, cámaras o algún otro dispositivo.
- Hackeo indirecto: El usuario confía sus datos del método de autentificación a terceros quienes pueden ser atacados.
- Phishing: Hace referencia a programas que se hacen pasar por entidades confiables para interceptar los datos que desean.

Seguridad en internet En la actualidad, el incremento constante de internet ha impactado directamente en la seguridad de la información que se maneja cotidianamente y por la mayoría de usuarios. Existen infinidad de sitios donde es aplicada la seguridad, ya que sin ésta, se verían afectados todos los usuarios en sus cuentas, pudiendo verse afectados desde un posible Identity theft (Robo de identidad), hasta la perdida de dinero real dado que la base de algunas de éstas páginas son E-Commerce, estas páginas implican el manejo de tarjetas de crédito, paypal, etc.

Uno de los puntos más críticos de la seguridad en Internet son las herramientas que interactúan de forma directa con los usuarios. Es común escuchar sobre fallas en los sistemas de protección de los servidores más frecuentemente utilizados, por ejemplo Apache, NGINX, IIS, etc. O en los lenguajes de programación en que son escritas las aplicaciones [24]. Sin embargo, la vulnerabilidad más grande dentro de un sistema, son los ataques directos a los usuarios finales durante la autentificación.

Una de las técnicas de autentificación que actualmente se usa es "recordar la sesión" usando las "cookies", en la siguiente sección, nos adentraremos en definir qué son las cookies y exponer sus vulnerabilidades.

2.4. Cookies.

Durante la navegación por internet, la información sobre la computadora puede ser colectada y almacenada. Ésta puede ser de carácter general sobre el equipo y puede ser también información más específica sobre los hábitos de navegación del usuario, toda esta información guardada se le conoce como Cookies.

A continuación se muestran los diferentes tipos de cookies que existen para los navegadores.

- **Cookies propias:** Las cookies se gestionan desde el terminal o dominio de un mismo editor.
- **Cookies de terceros:** Las cookies no son enviadas por el propio editor, sino por otra entidad.
- **Cookies de sesión:** Los datos recabados sólo se recogen mientras el usuario está navegando por la página web.
- **Cookies persistentes:** Los datos continúan almacenados en el terminal y se puede acceder a ellos durante un periodo de tiempo determinados.
- **Cookies técnicas:** Permiten controlar el tráfico y la comunicación de datos.
- **Cookies de personalización:** Dejan a los usuarios acceder según algunas características propias que se recogen (navegador, idioma, etc.).
- **Cookies de análisis:** Recogen datos sobre el comportamiento de los usuarios y permiten elaborar un perfil de usuario.
- **Cookies publicitarias:** Recogen datos sobre la gestión de los espacios publicitarios.

Las cookies persistentes son aquellas que se almacenan en el equipo para que las preferencias personales puedan ser retenidas, ayudan a los sitios web a recordar tu información y ajustes cuando los visitas más adelante. Esto conlleva un acceso más rápido y sencillo ya que, por ejemplo, no se tiene que iniciar sesión de nuevo. Además de la autentificación, otras páginas web tienen más funciones para las cookies permanentes, como: selección de idioma, selección de tema, preferencias de menú, marca-páginas internos de la web, o favoritos. Muchos navegadores pueden ajustar el periodo de tiempo en que las cookies persistentes deben ser almacenadas. [31]

Gracias a las cookies persistentes, las direcciones de correo electrónico aparecen por default cuando se abre el correo electrónico, o en páginas de inicio personalizadas cuando se visita en línea un comercio. Si un atacante obtiene acceso puede recopilar información personal del usuario través de estos archivos y poder robar toda información del usuario. Es fácil acceder a estas cookies y obtener fácilmente la información del usuario, por lo que es necesario que el usuario nunca deje vulnerable esta información o en su

debido caso borrar cookies al término de cada sesión. Existen diferentes funcionalidades para las cookies, una de las más importantes es la funcionalidad de seguridad, ya que contiene información importante de los usuarios [31]. A continuación se muestran las diferentes funcionalidades de las cookies.

- **Preferencias:** Sirven para que la página se visualice atendiendo a los gustos del usuario, como por ejemplo idioma, región o tamaño de textos.
- **Seguridad:** Se encargan de autenticar a los usuarios y evitar el uso fraudulento de las credenciales por parte de terceros.
- **Procesos:** Son utilizadas para el correcto funcionamiento de la página en el navegador.
- **Publicitarias/Estadísticas:** Se usan para que la publicidad que se muestre sea personalizada.
- **Estados de la sesión:** Obtienen información del comportamiento del usuario en una página web, como por ejemplo el tiempo que pasa en una página, los "clicks" que realiza o la publicidad que le aparece.

Una vez entendido que es la autenticación y el uso que se le puede dar a las cookies, procedemos a exponer como la criptografía es de gran ayuda en la seguridad en internet y como la usaremos para este nuevo método de autenticación.

2.5. Introducción a la Criptografía.

2.5.1. Criptología.

Para comprender que es la criptografía, es necesario que comprendamos qué es la "*Criptología*", palabra que proviene del griego «*kryptós*» (oculto) y «*logos*» (estudio). Según la Real Academia Española significa 'estudio de los sistemas, claves y lenguajes ocultos o secretos', sin embargo, brindándole un contexto a esta definición decimos que es el arte y ciencia que se encarga de diseñar sistemas para ocultar mensajes, y buscar la manera de romper dichos sistemas [4].

La criptología contiene dos ramas, las cuales son: el criptoanálisis y la criptografía. Ésta última es de vital importancia en este trabajo terminal, por lo que a continuación se explicará qué es, su historia, sus objetivos y sus usos que tiene esta rama en la actualidad.

2.5.2. Criptografía.

”*Criptografía*”, palabra proveniente del griego «*kryptós*» (oculto) y «*graphos*» (escribir), es definida por la Real Academia Española como ’el arte de escribir con clave secreta o de un modo enigmático’. Nuevamente, la definición de la RAE nos da un panorama general de lo que trata esta rama de la criptología, sin embargo, en la actualidad tenemos definiciones más extensas y precisas que nos ayudan a entender las funciones de este arte.

A continuación, se presentan dos definiciones de la criptografía, cabe mencionar que estas definiciones están orientadas al uso de la criptografía en la informática y las telecomunicaciones actualmente.

Jorge Ramírez Aguirre nos brinda la siguiente definición en su libro ’Seguridad informática y criptografía’ [2].

”Rama inicial de las matemáticas y en la actualidad también de la informática y la telemática, que hace uso de métodos y técnicas con el objeto principal de cifrar, y por tanto proteger, un mensaje o archivo por medio de un algoritmo, usando una o más claves.”

Finalmente, Menezes, Van Oorschot y Vanstone, no brindan en su libro una definición formal de lo que es la criptografía (traducción) [19].

”Estudio de técnicas matemáticas relacionadas con los aspectos de la seguridad de la información tales como la confidencialidad, la integridad de datos, la autenticación de entidad y del origen de datos. La criptografía no comprende sólo a los medios para proveer seguridad de información, sino a un conjunto de técnicas.”

A elección del lector elegir aquella definición que le convenza más, nosotros una vez finalizado la exposición de estas definiciones de criptografía, continuaremos con una breve remembranza de la historia de esta disciplina.

En Egipto hace 4000 años, tuvo su primera aparición la criptografía, cuando un maestro egipcio escribió la historia de su señor utilizando jeroglíficos poco comunes tratando de imprimir cierta jerarquía. Este primer acercamiento a la criptografía, utilizaba las técnicas de sustitución y transposición de símbolos de una manera similar a la base del concepto general de cifrado. Posteriormente, las antiguas civilizaciones occidentales comienzan a adoptar estas técnicas para mantener determinada información oculta, principalmente con propósitos militares, diplomáticos y religiosos. Mientras la criptografía crecía alrededor del mundo, el criptoanálisis también lo hacía, con el objetivo de hallar el mensaje original a partir de un mensaje cifrado, sin conocer el

método utilizado [6] [17].

En la historia conocida después de lo antes mencionado, existe un punto crucial en el desarrollo de la criptografía tal y como la conocemos hoy en día hasta la llegada de las computadoras. Este punto fue la Segunda Guerra Mundial, en donde se construyeron máquinas de cifrado mecánicas y electromecánicas que aceleraban el proceso de cifrado y descifrado. Los alemanes desarrollaron la famosa máquina 'Enigma', que precisamente mediante unos rotores automatizaba el proceso de cifrado y descifrado de mensaje, brindándole al ejército una ventaja considerable en la inversión de tiempo en la comunicación.

2.5.2.1. Criptografía moderna.

En la actualidad, el término '*criptografía moderna*' hace alusión al desarrollo de esta ciencia en las áreas de la teoría de la información y las comunicaciones. Claude Shannon, considerado por muchos como el padre de la criptografía matemática, en su libro "Sistemas secretos" estableció las bases para las implementaciones de los algoritmos actuales a mediados de los años 50s [17].

En los años 70s, el público general tuvo acceso al trabajo de Claude, además surgió la llegada de las computadoras y la publicación el primer borrador del algoritmo de criptografía simétrica DES, el cual fue el primer algoritmo público, basado en técnicas matemáticas y criptográficas modernas. Todo ello representó los cimientos para un rápido crecimiento en la criptografía, hasta eventualmente llegar a otro hecho sumamente relevante que determinó gran parte de las transacciones que realizamos hoy en día en internet. Dicho hecho fue el artículo de las nuevas direcciones de criptografía hecho por Whitfield Diffie y Martin Hellman, el cual trataba de un nuevo método para distribuir llaves, que eventualmente se llamaría criptografía asimétrica.

2.5.3. Objetivos de la criptografía.

Algunos de los objetivos que se busca con la implementación de la criptografía para la seguridad de la información son los siguientes:

- **Confidencialidad:** este objetivo, también conocido como privacidad de la información, implica mantener en secreto una determinada información, por tanto, sólo aquellas personas que estén autorizadas tendrán acceso a ella.

- **Autentificación:** este objetivo, implica hablar de la corroboración de la identidad de una entidad, por tanto, asegura que la entidad de donde la información es originada pueda ser identificada.
- **Integridad:** este objetivo asegura que determinada información no haya sido alterada por personas no autorizadas o por cualquier otro medio no conocido.
- **No repudio:** este objetivo previene que una entidad niegue un envío de información de un acuerdo preestablecido.

2.5.4. Usos de la criptografía.

Los usos que tiene la criptografía son muy variadas, dependiendo del ámbito donde se está aplicando. Las siguientes usos, son sólo algunas de los tantos que hay y provienen de distintos objetivos que tiene la criptografía aplicada a la seguridad de la información [17].

- **Autorización:** permiso concreto, de una parte o entidad, para el acceso o la realización de una tarea específica.
- **Validación:** proveer una autorización para el uso o la manipulación de información o recursos.
- **Control de acceso:** restricción de acceso a la información o recurso.
- **Certificación:** respaldo de información por una entidad externa de confianza.
- **Confirmación:** acuse de recibo a servicios que han sido dados.
- **Anonimato:** ocultamiento de la identidad de una entidad.

2.5.5. Criptografía simétrica y asimétrica.

Anteriormente en la historia de la criptografía, se hizo una rápida mención del nacimiento de estos dos métodos de cifrado, en esta sección se explicará más profundamente sus funciones con el fin de que el lector conozca un poco más y entienda porque hemos decidido utilizar determinado método para cumplir con los objetivos de este trabajo.

2.5.5.1. Criptografía simétrica.

En la criptografía simétrica, tanto el emisor como el receptor comparten una única llave secreta para cifrar y descifrar la información que se deseé transmitir. Esto implica que ambas partes de la comunicación deben tener un acuerdo antes de que se realice la comunicación. La seguridad de este tipo de algoritmos radica en mantener segura la llave secreta, por tanto, si ésta es revelada, cualquiera con acceso a ella puede descifrar el mensaje. Por estas razones, este tipo de criptografía puede ser visto como criptografía de llave privada". Algunos de los algoritmos más famosos de criptografía simétrica son: DES (Data Encryption Standard), TripleDES, AES (Advanced Encryption Standard) y IDEA (International Data Encryption Algorithm) [17]. En el esquema de la Figura 2.4, se muestran los pasos que sigue un protocolo de criptografía simétrica. Definamos 'A' como una entidad que pretende enviar un mensaje a otra entidad llamada 'B'. Luego entonces, ambas partes acordarán una 'Llave Secreta' con la que 'A' cifrará el mensaje utilizando un algoritmo establecido, mandando el resultado (Texto Cifrado) a 'B' que descifrará el mensaje con la misma llave y algoritmo que 'A'.

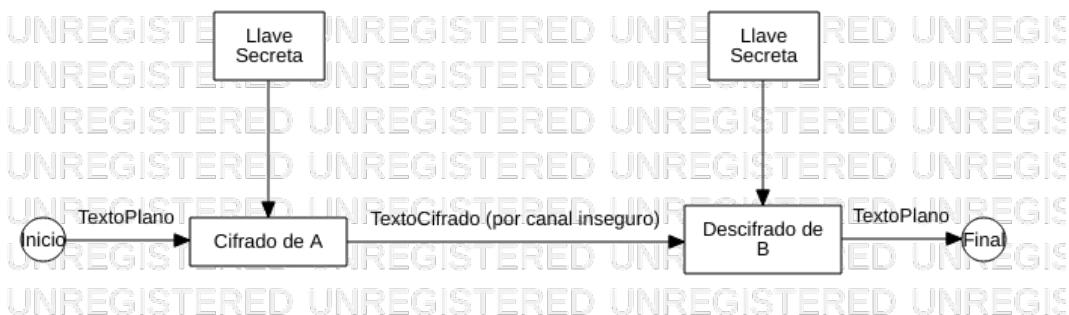


Figura 2.4: Esquema del protocolo de criptografía simétrica.

2.5.5.2. Criptografía asimétrica.

La criptografía de clave pública fue inventada en 1976 por los matemáticos Whitfield Diffie y Martin Hellman y es la base de la criptografía moderna. En los algoritmos de criptografía asimétrica, el receptor posee una llave pública y una llave privada para poder descifrar los mensajes. Las claves privadas deben ser conocidas únicamente por su propietario, mientras que la correspondiente clave pública puede ser dada a conocer abiertamente. Si un usuario quiere enviar a otro un mensaje de forma que sólo el receptor pueda entenderlo, lo codificará con la clave pública del receptor y éste utilizará su clave

privada, que solo él tiene, para poder leerlo. Dicho esto, podemos llamar llave de cifrado a la llave pública y llave de descifrado a la llave privada, siendo ambas totalmente diferentes una de la otra. Algunos de los algoritmos más famosos de criptografía asimétrica son: RSA y ElGamal [17].

La criptografía asimétrica está basada en la utilización de números primos muy grandes. Si multiplicamos entre sí dos números primos muy grandes, el resultado obtenido no puede descomponerse eficazmente, es decir, utilizando los métodos aritméticos más avanzados en las computadoras más avanzadas sería necesario utilizar durante miles de millones de años tantas computadoras como átomos existen en el universo. El proceso será más seguro cuanto mayor sea el tamaño de los números primos utilizados.

En el esquema de la Figura 2.5, se muestran los pasos que sigue un protocolo de criptografía asimétrica. Definamos 'A' como una entidad que desea enviar información a otra llamada 'B'. Luego entonces, 'B' enviará a 'A' su llave pública para que 'A' cifice la información utilizándola. Cuando la información (Texto Cifrado) haya viajado a través del canal inseguro para que 'B' la reciba, 'B' descifrará el Texto Cifrado con su llave privada.

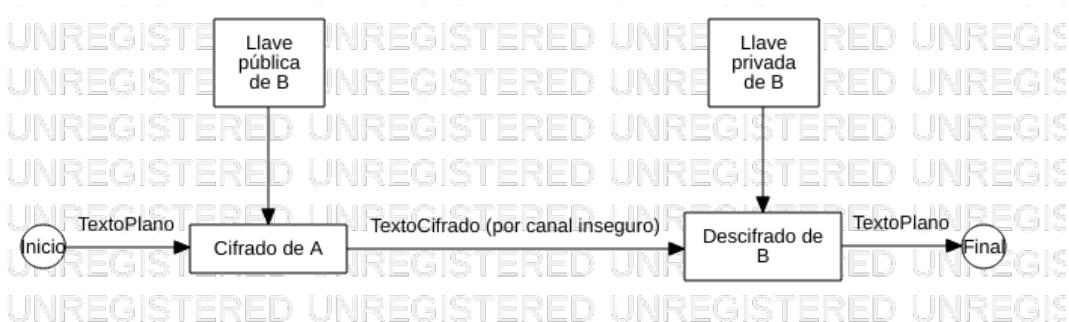


Figura 2.5: Esquema del protocolo de criptografía asimétrica.

Algoritmo RSA.

RSA es el algoritmo de cifrado asimétrico más popular en la actualidad. Creado por Ron Rivest, Adi Shamir y Leonard Adleman y publicado en el año 1977. El algoritmo es considerado seguro, en tanto sean utilizadas llaves de longitud suficientemente seguras (se siguen utilizando llaves de 1024 bits, pero ya se recomienda al menos una longitud de 2048). El algoritmo sirve tanto para cifrar y descifrar, así como también para la generación de firmas digitales. Es, en la actualidad, ampliamente utilizado en protocolos de comercio electrónico. La seguridad *RSA* está basada en la dificultad de realizar

el *factoreo* de números grandes. La llave privada y la pública son generadas o calculadas en función de un par de números primos, del orden de los 200 dígitos o más grandes aún [17].

Al describir ya concretamente al algoritmo, se establece que para la generación del par de llaves (Llave pública y privada) se deberán seleccionar dos números primos grandes aleatorios, p y q , y se calculará n como su producto:

$$n = pq$$

La llave de cifrado, e , será elegida también de manera aleatoria, tal que e y $(p - 1)(q - 1)$ sean primos relativos.

La llave de descifrado d será obtenida despejando la ecuación:

$$ed = 1 \bmod (p - 1)(q - 1)$$

En otras palabras, o mejor dicho, en otros símbolos:

$$d = e^{-1} \bmod ((p - 1)(q - 1))$$

Los números e y n componen la llave privada; el número d corresponde a la llave pública; p y q serán descartados pero no revelados.

A la hora de cifrar un mensaje m , éste deberá ser dividido en bloques más pequeños que n y cada parte del texto-cifrado, c , será obtenida mediante:

$$c_i = m_i^e \bmod n$$

Para el descifrado, cada parte o bloque del texto-cifrado se tomará para calcular:

$$m_i = c_i^d \bmod n$$

El patrón con el que se genera el código *Chaffing* no puede viajar a través de la red visible para cualquier entidad que quiera obtener dicha petición, por lo que, debemos cifrarlo con algún algoritmo confiable.

El algoritmo RSA nos proporciona esa seguridad, debido a que es un cifrado asimétrico con el cual podemos cifrar el patrón con la llave pública del servicio. Una vez que la petición cifrada llegue al servicio, este será capaz de descifrar dicho mensaje con su llave privada, para así poder ver el mensaje original.

2.5.6. Criptografía a nivel de aplicación.

La criptografía a nivel de aplicación se entiende como aplicaciones o programas informáticos que hacen uso de diferentes técnicas criptográficas. Al hablar de criptografía en el nivel de aplicación, también podría considerarse a los protocolos criptográficos de alto nivel, los cuales determinan como han de comunicarse ambas partes, que algoritmos usar, define formatos, etc [17].

2.5.6.1. SSL/TLS.

Secure Sockets Layer (SSL) provee servicios de seguridad entre la capa TCP y las aplicaciones que hacer uso de esa capa. Actualmente, la sucesora de SSL es TLS (Transport Layer Service), sin embargo, lo acuñado que está el término SSL hace que se use indistintamente para referirse a TLS, aunado a ello, las diferencias entre la última versión de SSL (SSL3.0) y la primera versión de TLS (TLSv1) son menores, por lo que en el desarrollo de este reporte, utilizaremos el término SSL/TLS.

SSL/TLS provee entonces confidencialidad, lográndola con criptografía asimétrica y controlando la integridad de los datos utilizando un MAC (Message Authentication Code).

El proceso de comunicación del protocolo establece, como primer paso, la negociación de ambas partes de los algoritmos a utilizar. Luego, procede al intercambio de llaves públicas y a la autenticación basada en certificados digitales para, finalmente, cifrar de manera simétrica los datos o información a transferir [17].

En nuestro trabajo, usaremos SSL/TLS para brindar confidencialidad al canal de comunicación entre la extensión y el servidor autenticador. Esto se explicará más a detalle en el análisis del Componente II.

2.5.6.2. OpenSSL

OpenSSL es un proyecto de código abierto que implementa funciones criptográficas sin limitaciones dentro de una librería y que provee diversas herramientas útiles. OpenSSL actualmente implementa SSL2.0, SSL3.0 y TLSv [17].

Dentro de las herramientas que tiene se encuentran:

- Crear y manejar llaves privadas, públicas y parámetros.

- Realizar operaciones criptográficas de llave pública.
- Calcular hash de algún mensaje.
- Cifrar y descifrar con algoritmos simétricos.
- Crear certificados X.509 (CSRs y CRLs).

Esta última herramienta, es la que usaremos para este trabajo terminal. Se creará un certificado de cada usuario a partir de sus datos de inicio de sesión para autenticarlo en los servicios web en donde quiera acceder. Esto se explicará más a detalle en el análisis del Componente II.

Ahora que se ha expuesto el uso de la criptografía en este trabajo, procedemos a platicar acerca del método *Chaffing and Winnowing* y cómo se implementará en este trabajo.

2.6. Chaffing and Winnowing.

2.6.1. Historia

Chaffing and Winnowing es una técnica que logra confidencialidad sin usar ningún proceso de cifrado para el envío de datos sobre un canal inseguro. El nombre **Chaffing and Winnowing** el nombre proviene de la agricultura: Déspués de que el grano ha sido cosechado y trillado es mezclado con paja fibrosa no comestible. La paja y el grano son separados por el movimiento de las hojas y la paja es descartada. Ésta técnica fue creada por Ron Rivest y fue publicada en un artículo en línea el 18 de Marzo de 1998 [23]. Aunque parece ser similar a un cifrado tradicional o esteganografía, chaffing and winnowing no puede ser clasificado como uno de ellos.

Ésta técnica permite el envío de datos evitando la responsabilidad del cifrado de su contenido. Cuando se usa chaffing and winnowing, el emisor transmite el mensaje sin cifrar (texto plano). Aunque el emisor y el receptor comparten una llave, ellos la usan sólo para autenticar. Sin embargo, una tercera parte puede hacer su comunicación confidencial durante el envío simultáneo de mensajes especialmente mensajes diseñados a través del mismo canal.

2.6.2. ¿Qué es Chaffing and Winnowing?

Chaffing and Winnowing es un nuevo esquema establecido por Rivest en 1998. Este esquema ofrece confidencialidad para el contenido de un mensaje sin involucrarse con cifrado ni esteganografía [17].

El proceso **Chaffing** no hace uso de un cifrado por lo que no tiene una "clave de cifrado". Este proceso consiste en agregar paquetes inválidos (Información innecesaria) al mensaje a enviar, haciendo que el mensaje viaje seguro a la vista de todos los posibles "atacantes".

El proceso de **Winnowing** no emplea algún tipo de cifrado, por lo que al igual que el proceso chaff no tiene una "clave de descifrado". Intentando regular la confidencialidad que provee un cifrado damos paso a la esteganografía y el proceso de winnowing [23].

Existen dos partes en el envío de mensajes con winnowing: Autentificación (Agregando MACs) y agregando paquetes chaff. Nosotros nos enfocaremos mas al uso de paquetes chaff para el envío seguro de información, ya que, el receptor es quien remueve los paquetes chaff para obtener el mensaje original.

Los siguientes esquemas explican como es que se lleva a cabo el proceso de **Chaffing and Winnowing** en diferentes escenarios.

Escenario 1: Alice se está comunicando con Bob en un solo camino de comunicación sobre un canal inseguro y Charles agrega los paquetes de Chaff.

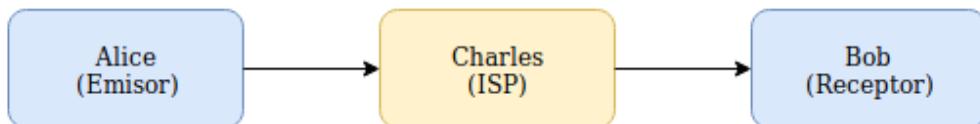


Figura 2.6: Charles agrega los paquetes inválidos.

En el escenario anterior Alice y Bob se están comunicando mutuamente por un canal de comunicación no seguro, en donde son enviados paquetes no cifrados. Alice y Bob comparten la llave de autentificación la cual será usada para el proceso de autentificación. Cuando Alice envía un mensaje a Bob, su mensaje es autenticado de su lado y es enviado a Charles antes de ser enviado a Bob. Charles agrega los paquetes chaff a la secuencia transmitida por Alice, al agregar los paquetes chaff, Charles provee confidencialidad para la comunicación entre Alice y Bob. Pero donde Charles no conoce la llave secreta compartida entre Alice y Bob. Por lo que el proceso de chaffing no necesita ningún conocimiento de la llave secreta de autentificación compartida.

Escenario 2: Alice se comunica con Bob en un camino de comunicación inseguro y en el cual Charles no agrega los paquetes chaff si no que multiplexa los flujos de las dos partes (David y Alice). Este escenario es diferente al anterior, ya que se multiplexa el flujo de datos de Alice y Bob con el flujo de datos de David y Jane, y cuando el paquete llega a Bob el flujo de paquetes de David hacia Jane es el chaff de Bob y es descartado y vice versa para Jane.

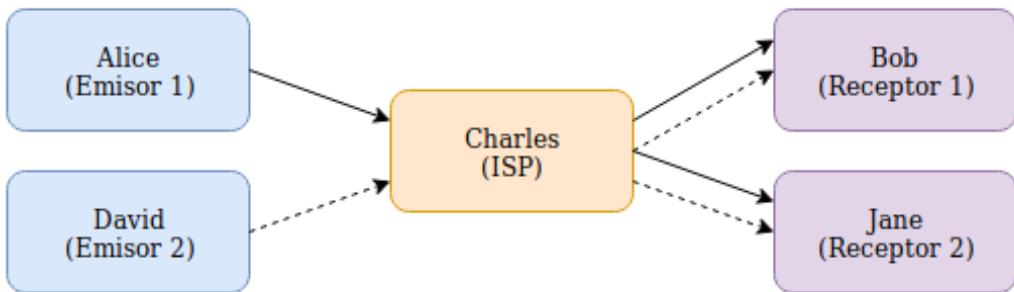


Figura 2.7: Charles no agrega los paquetes pero multiplexa los flujos.

Escenario 3: Alice se comunica con Bob en un canal de comunicación inseguro y Alice no agrega los paquetes chaff. En este escenario, Alice desarrolla la autenticación de sus mensajes, por lo que Alice aplica chaffing para autenticar los mensajes y producir una secuencia de paquetes que serán transmitidos a Bob por la vía de Charles. Bob lleva a cabo el proceso de winnowing para recuperar el mensaje original.

2.6.3. Objetivo de Chaffing and Winnowing

El objetivo de seguridad del esquema de chaffing-and-winnowing es proporcionar privacidad en un entorno simétrico. Desde un punto de vista de seguridad, este esquema debe tratarse simplemente como un esquema de cifrado simétrico. Hay algunos procesos de "cifrado" que toman un mensaje y crean un "texto cifrado", y algún proceso de "descifrado" toma el texto cifrado y recupera el mensaje, ambos operando bajo una clave secreta en común. (Para el esquema Chaffing and Winnowing es la clave para el MAC). Estos procesos no se implementan de manera "habitual", pero, de manera abstracta, deben existir, de lo contrario no se logra la privacidad [3] [10].

"No es una propiedad de seguridad novedosa, sino un conjunto novedoso de

restricciones en los procesos dirigidos a lograr una propiedad de seguridad estándar”

”Encontrar-luego-adivinar”. Extensión más directa al caso simétrico de la noción de indistinguibilidad.

Haciendo uso de **Chaffing and Winnowing** se asegura que los adversarios no obtengan información del mensaje transmitido a lo largo de un canal de comunicación inseguro entre dos partes.

Rivest propone un esquema, el cual cuenta con tres partes principales [23].

1. **Autentificación** Es el proceso de descomponer el mensaje original en un paquete más pequeño y complementar cada paquete con un código de autentificación de mensaje (MAC).
2. **Chaffing** Es el proceso de agregar paquetes inválidos (Chaff packets).
3. **Winnowing** Es el proceso de remover paquetes Chaff para obtener el mensaje original en texto plano.

2.6.4. ¿Cómo funciona?

El esquema de Chaffing and Winnowing deja que cada paquete conste de:

- Un número de serie
- Contenido del paquete
- Código de autentificación del mensaje

Cuando son enviados los paquetes, el mensaje con el texto plano se descompone en pequeños paquetes los cuales contienen datos y el tamaño del paquete original. Entonces, el emisor (Alice) usa el algoritmo de **código de autentificación de mensaje** (MAC) para generar el valor MAC para ser agregado al paquete y el cual se basa en el número de serie, contenido del paquete y la llave autentificación. La Figura 2.8, muestra la salida del paquete después del proceso de autentificación.

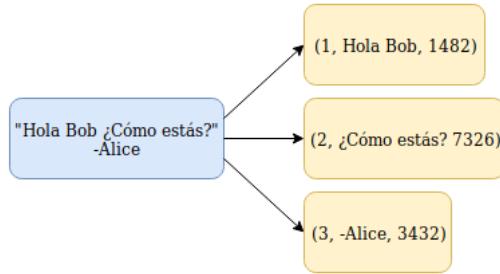


Figura 2.8: Secuencia de Chaffing después del proceso de autentificación.

Esta secuencia de paquetes es enviada a Charles (ISP) para llevar a cabo el proceso de Chaffing. Charles agrega paquetes chaff a la secuencia de paquetes antes de ser enviados por medio del canal de comunicación y ser recibidos por Bob.

Existen dos maneras donde Charles puede enviar la secuencia de chaff hacia Bob. La primera es enviando aleatoriamente mezclados los paquetes chaff para formar una secuencia y la otra manera es enviarlos de manera ordenada por el número de serie seguido del contenido del mensaje. En la Figura 2.9, se muestra cómo es el proceso de chaff en esta secuencia.

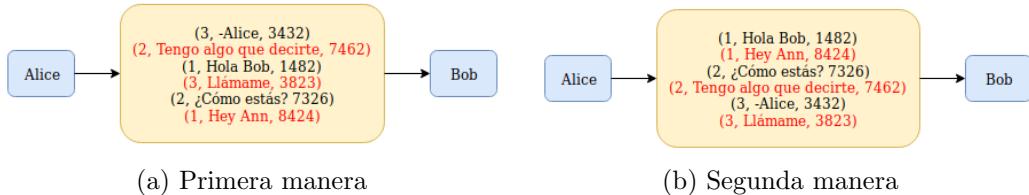


Figura 2.9: Las dos maneras para el proceso de chaff pueden ser utilizadas. Los paquetes chaff son los mensajes de color rojo.

Una vez que la secuencia de chaff llega a Bob, el último proceso es Winnowing. Bob determina la secuencia del mensaje que es válida del paquete chaff usando una función hash para el contenido de cada paquete y la llave de autentificación para re-calcular el MAC y compararlo contra el MAC del paquete recibido, si la comparación falla, el paquete chaff es descartado. Si la comparación es valida, entonces el paquete es parte del mensaje original. En la Figura 2.10, se muestra el proceso completo de Chaffing and Winnowing [23].

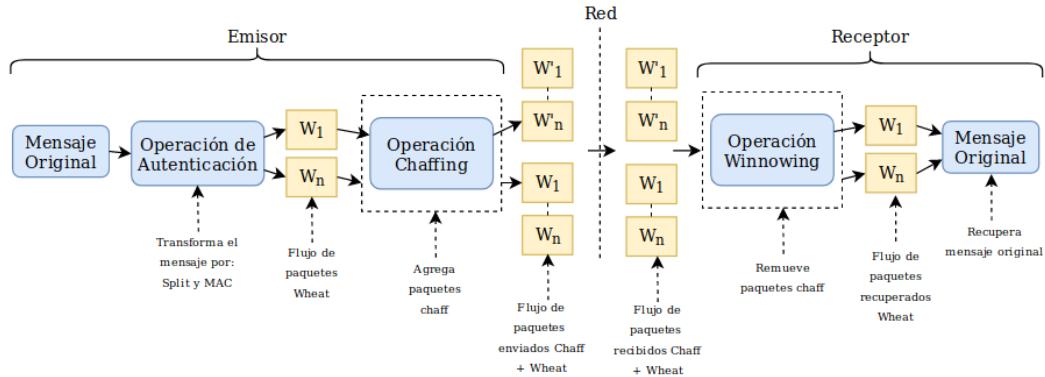


Figura 2.10: Visión general del proceso Chaffing and Winnowing.

2.6.5. Propiedades de Chaffing and Winnowing

- La técnica de Chaffing and Winnowing no depende de la fuerza del esquema de cifrado para proporcionar confidencialidad debido al hecho de que es muy difícil distinguir la información útil de los paquetes chaff sin la clave secreta. Por lo tanto, la dificultad de distinguir la información útil del chaff proporciona confidencialidad al esquema.
- La operación de Chaffing puede ser realizada por un tercero, ya que la clave secreta compartida no es necesaria en el proceso del mismo.
- Los paquetes de Chaff no tienen que contener datos aleatorios, ya que uno podría usar un mensaje válido con una clave secreta diferente para hacer el paquete de Chaff. Cuando el receptor recibe esos paquetes de Chaff, se verán como paquetes de Chaff, ya que la clave que se usa para volver a calcular el Chaff es diferente de la que los hace.

2.6.6. All-or-Nothing and the Package Transform (AONT)

All-or-Nothing and the Package Transform es una variación dentro de la técnica Chaffing and Winnowing, donde se mejora la eficiencia de su esquema original. AONT es la transformación de pre-procesamiento que permite a las partes enviar más datos (en términos de bit) por paquete en lugar de solo uno. Este pre-procesamiento es una transformación sin cifrado que toma el mensaje de texto sin formato y produce un mensaje empaquetado que

luego se procesa de la manera normal de Chaffing and Winnowing [16]. Las definiciones de la transformación AONT son las siguientes:

1. El algoritmo de transformación es **reversible**: Dado el bloque de mensaje transformado, el receptor puede obtener el mensaje de texto sin formato original.
2. El algoritmo de transformación y su inverso son **computables** de manera eficiente: Lo que significa que es computacionalmente factible recrear el texto original dada la llave privada y recibir todos los paquetes con éxito.
3. La transformación no es **computacionalmente factible**: Esto significa que si se ha recibido parte del paquete de la transmisión, cualquiera que esté intentando leer el mensaje no puede hacerlo ya que la transformación **AONT** requiere que se reciba todo el mensaje, de lo contrario no entrega nada.
4. La transformación es una **técnica sin cifrado**: La técnica de preprocesamiento no tiene llaves y no hay una llave secreta compartida involucrada en la operación. Cualquier persona que haya recibido todos los mensajes transformados del paquete puede recuperar el mensaje de texto original.

¿Cómo funciona AONT?

Supongamos que el mensaje de entrada es el siguiente: m_1, m_2, \dots, m_n . Seleccionamos una llave aleatoria K' el cual se usará para la función del paquete de transformación.

Se calcula la secuencia transformada $m'_1, m'_2, \dots, m'_{s'}$ para $s' = s + 1$ como se muestra a continuación:

Tenemos:

$$m_i \otimes E(K', i) \text{ for } i = 1, 2, 3, \dots, s$$

También:

$$m'_{s'} = K' \otimes h_1 \otimes h_2 \otimes \dots \otimes h_s$$

Donde:

$$h_i = E(K_0, m'_i \otimes i) \text{ for } i = 1, 2, \dots, s$$

Donde K_0 es una llave conocida pública fija.

Para que el receptor en el otro extremo obtenga el K_0 , el cual es la llave para el uso de **AONT**, el receptor realiza el siguiente cálculo:

$$K' = m'_s \otimes h_1 \otimes h_2 \otimes \dots \otimes h_s$$

$$m_i = m'_i \otimes E(K', i) \text{ for } i = 1, 2, \dots, s$$

AONT toma el mensaje de texto sin formato de entrada y los transforma, luego crea un bloque para almacenar los mensajes transformados antes de pasar al proceso de autenticación. Despues, se genera el paquete Chaff (la cantidad de paquetes Chaff no tiene que ser igual a los paquetes de la información útil).

Esta técnica produce una menor sobrecarga que la sugerencia número 1. El AONT ofrece más confidencialidad al esquema de Chaffing and Winnowing, ya que el adversario debe recibir todo el bloque de mensajes de transformación e identificar correctamente todo el paquete de la información útil para obtener el mensaje de texto original. La Figura 2.11, muestra la descripción general de Chaffing y Winnowing si se agrega la función AONT [16].

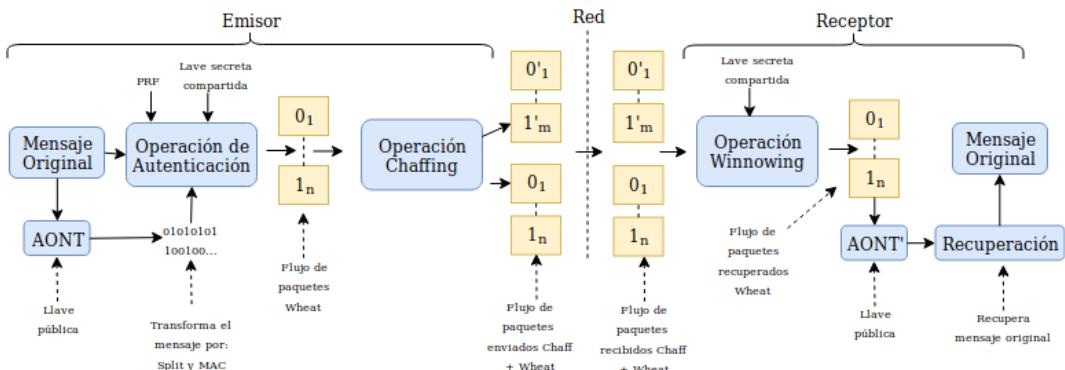


Figura 2.11: Proceso de Chaffing and Winnowing junto con AONT.

¿Cómo AONT puede hacer la diferencia?

1. Requiere menos ancho de banda al transferir paquetes, ya que se pueden transferir más bits en un paquete en lugar de un bit por paquete.
2. Los paquetes Chaff son más fáciles de generar, ya que AONT transforma el mensaje de texto plano en bits aleatorios.

3. La distinción entre Chaffing and Winnowing es más difícil: Si el adversario va a ejercer fuerza bruta en los paquetes, la tarea se ralentizará por el factor del número de bloque de mensajes. Dado que el bloque de mensaje de información adicional se mezcla aleatoriamente dentro de los flujos de paquetes de Chaffing and Winnowing, sin saber que es muy difícil que el bloque adicional proporcione la posibilidad de elegir el bloque de mensaje correcto de los paquetes para obtener el texto plano original.

2.6.7. Comparando Chaffing and Winnowing contra Cifrado y Esteganografía

En esta sección explicaremos porque Chaffing and Winnowing no puede ser clasificado como una técnica de cifrado o Estenografía.

2.6.7.1. Chafing and Winnowing vs Cifrado

Nosotros podríamos clasificar Chaffing and Winnowing como un método de cifrado, pero volvamos a recordar el principio de un Cifrado. El principal objetivo de un cifrado es ocultar el mensaje en texto plano de tal manera que oculta su contenido con el uso de una clave de cifrado para el texto cifrado. Por otro lado, en el esquema original de Chaffing and Winnowing, una llave compartida es usada con el fin de autentificar la validación de los paquetes ya sea del emisor o del receptor. Además, Chaffing and Winnowing no hace uso de ninguna técnica de cifrado para ocultar el contenido de un mensaje y que nadie pueda ver dicho mensaje, solo aquellos con la llave correspondiente pueden determinar que paquetes contienen la información valida. En la figura 2.11, se muestra como se puede ver el esquema Chaffing and Winnowing como una técnica de cifrado.

Chaffing y Winnowing pueden verse como **un tipo especial de esquema de cifrado simétrico**, ya que la operación **chaffing** es similar al "proceso de cifrado". En la operación de chaffing, el texto cifrado se crea para producir un paquete de la información útil no válido que se envía al receptor. Luego, el receptor realiza el "proceso de descifrado", que implica descartar el paquete de desperdicios y recuperar el mensaje original. Ambas operaciones operan bajo una llave secreta común que se usa para derivar el valor MAC.

Pero la diferencia es, *Chaffing y Winnowing* dos partes que no buscan lograr la confidencialidad. El emisor comparte una clave secreta con el re-

ceptor para que el receptor pueda usar la clave secreta para autenticarse (si se afirma que el mensaje recibido proviene del remitente deseado). Pero la ganancia de confidencialidad proviene de la dificultad de distinguir el paquete Chaff del paquete de la información útil. Mientras que en el cifrado, la clave se utiliza para lograr la confidencialidad mediante la creación de texto cifrado que oculta el contenido del mensaje de personas [23].

Chaffing y Winnowing junto con el esquema AONT, el esquema en sí es muy parecido al cifrado, excepto que la clave que se usa en la transformación AONT, se elige aleatoriamente cada vez en lugar de fijarla. Además, el último bloque de mensajes es exclusivo o de la clave y todo el hash del bloque de mensajes está allí para garantizar que cualquier modificación en el bloque de mensajes cambiará la clave K' calculado por el receptor. Por lo tanto, el último bloque de mensajes $m'_{s'}$ está allí solo con el propósito de autenticación. Por lo tanto, Chaffing y Winnowing con el esquema AONT no pueden ser clasificados bajo cifrado [16].

2.6.7.2. Chaffing and Winnowing vs Esteganografía

La esteganografía trata de cómo ocultar, dentro de un mensaje público, información secreta. La agregación de información 'extra' es también un secreto, es decir, nadie externo a la comunicación sabe que en ese mensaje público se ha agregado información [17]. Un ejemplo de esta técnica de cifrado, se puede visualizar claramente en la utilización de tinta invisible en cartas. El emisor escribe una carta común y corriente con tinta visible, pero además, escribe información secreta con tinta invisible. Luego entonces, el receptor, aplicando el método correspondiente, descubrirá la información mandada con tinta invisible, pero agentes externos, ni siquiera saben la existencia de dicha información. En la actualidad, la esteganografía es muy utilizada para ocultar información en archivos de imágenes.

Para algunas personas, Chaffing and Winnowing puede ser clasificado como una técnica esteganografía. Sin embargo, el objetivo principal de la esteganografía, como se mencionó antes, es el de ocultar el mensaje original dentro de otro mensaje, por lo tanto, nadie aparte del emisor y el receptor sabrá que hay un mensaje oculto. Contrario a Chaffing and Winnowing, en donde cualquiera puede ver el contenido del mensaje, ya que este método no trata de esconderlo de los posibles atacantes. Otra diferencia es que en esteganografía el emisor tiene que ocultar el mensaje el mismo, mientras que en Chaffing and Winnowing no necesariamente es así, ya que una "tercera

parte” puede hacerlo [18].

Por lo tanto, Chaffing and Winnowing no puede ser considerado como esteganografía.

Para nuestro trabajo terminal usaremos *Chaffing and Winnowing*, proponiendo así un nuevo método de autentificación para servicios web.

Capítulo 3

Análisis.

3.1. Estudio de Factibilidad.

El estudio de factibilidad es un instrumento que sirve para orientar la toma de decisiones en la evaluación de un proyecto y corresponde a la última fase de la etapa pre-operativa dentro del ciclo del proyecto. Se formula con base en información que tiene la menor incertidumbre posible para medir las posibilidades de éxito o fracaso de un proyecto, apoyándose en él se tomará la decisión de proceder o no con su implementación. Este estudio establecerá la viabilidad, si existe, del trabajo.

- Factibilidad Técnica: Hace referencia a los recursos como herramientas, conocimientos, habilidades, experiencia, etc. que son necesarios para efectuar las actividades del trabajo terminal.
- Factibilidad Operativa: Se refiere a los recursos necesarios para llevar a cabo los procesos de forma eficiente , depende de los recursos humanos.
- Factibilidad Económica: Consiste en los recursos financieros necesarios para llevar a cabo la elaboración de este trabajo.

3.1.1. Factibilidad Técnica

En esta parte explicaremos detalladamente las tecnologías que usaremos. Para la elección de estas herramientas fue necesario investigar las tecnologías que más se usan en la actualidad, además de ver las características y equipos de cómputo con los que contamos actualmente.

Factibilidad Técnica	
Sistema Operativo	Multiplataforma
Navegador Web	Google Chrome
Lenguaje de Programación	JavaScript
Servidor	Apache 2.0

Cuadro 3.1: Herramientas de Software a utilizar

Además de las herramientas de software a utilizar, es necesario mencionar el equipo de hardware que utilizaremos tanto para desarrollar como para probar e implementar cada uno de los prototipos que se mencionarán a lo largo de este trabajo terminar, el cual es:

Equipo de hardware [1]	
Marca	DELL
Modelo	Inspiron 5567
Procesador	Intel Core i7 7gen
Tarjeta de video	Radeon (TM) R7 M445
Memoria RAM	16 GB
Disco Duro	1 TB

Cuadro 3.2: Equipo de hardware a utilizar [1]

Equipo de hardware [2]	
Marca	Asus
Modelo	X550VC
Procesador	Intel Core i5
Tarjeta de video	NVidia GForce 720
Memoria RAM	12 GB
Disco Duro	1 TB

Cuadro 3.3: Equipo de hardware a utilizar [2]

Equipo de hardware [3]	
Marca	HP
Modelo	Pavilion g4
Procesador	Intel Core i3
Tarjeta de video	Intel Sandybridge Mobile
Memoria RAM	6 GB
Disco Duro	500 GB

Cuadro 3.4: Equipo de hardware a utilizar [3]

Junto con las herramientas de hardware y software a utilizar es necesario mencionar una serie de servicios básicos que son relevantes para el desarrollo de este trabajo terminal como lo son:

- Luz Eléctrica
- Agua Potable
- Internet
- Papelería en general

Estos servicios forman parte de la factibilidad técnica ya que sin ellos no se podría realizar este trabajo terminal y por eso mismo generan un costo, dicho costo se menciona en la Factibilidad Económica.

3.1.2. Factibilidad Operativa

Los recursos operativos de este trabajo terminal se calcularon con base en los recursos humanos con los que se cuenta y un análisis de las horas que el personal estará en operación trabajando sobre éste, el cual se muestra a continuación:

Horas a trabajar en el desarrollo del trabajo terminal						
Mes	No. de Días	Sábado y Domingo	Días hábiles	Horas de trabajo por día	Horas Totales	Días laborables (8 hr.)
Enero	31	8	9	2	18	2
Febrero	28	8	19	2	38	4
Marzo	31	10	20	2	40	5
Abril	30	10	15	2	30	3
Mayo	31	8	18	2	36	4
Junio	30	10	8	2	16	2
Agosto	31	9	12	2	24	3
Septiembre	30	10	16	2	32	4
Octubre	31	10	20	2	40	5
Noviembre	31	8	18	2	36	4

Cuadro 3.5: Relación de horas de trabajo estimadas para la realización de este trabajo terminal

Con esto podemos concluir que contamos suficiente tiempo para el desarrollo de este trabajo terminal, ya que las horas totales de trabajo están contempladas para cada uno de los integrantes del equipo

3.1.3. Factibilidad Económica

Luego de haber realizado el estudio de factibilidad técnica así como el operacional es necesario tomar en cuenta un estudio de factibilidad económica el cuan desglosará todo el gasto económico realizado para la elaboración de este trabajo terminal:

- Capital Humano: Se tienen contemplados aproximadamente 36 días laborales, es decir 288 horas para la elaboración de este trabajo terminal en el cual participaremos los cuatro integrantes
- Capital Técnico: Se cuentan con las instalaciones de la escuela, así como las viviendas de cada uno de los integrantes y los equipos de cómputo correspondientes.

En cuanto a los costos monetarios de todo el trabajo terminal se tiene lo siguiente:

- Servicios
En cuando a los servicios se considera un gasto mensual aproximado

de \$1,600.00 que al multiplicarlo por todo el tiempo de elaboración tenemos \$ 16,000.00.

- Software

En este caso durante todo el trabajo terminal usaremos herramientas gratuitas y la mayoría de software libre por lo que no dedicaremos una parte monetaria en el gasto de este tipo.

- Hardware

En este caso y como se mencionó anteriormente utilizaremos los equipos de cómputo personales de cada integrante lo que da un costo aproximado total de \$ 35,000.00.

- Recursos Humanos

Estamos estimando un gasto de \$80,000.00 por cada integrante para la elaboración de este trabajo terminal por lo que se genera un gasto total de \$320,000.00

Por lo que el costo final del desarrollo de este trabajo terminal es:

\$371,000.00

Conclusión Tras analizar todo este trabajo terminal y cada una de las partes del estudio de factibilidad es pertinente decir que los integrantes no contarán con el apoyo financiero antes mencionado y que el hardware actualmente ya es propiedad de los integrantes, por lo que el trabajo terminal se califica como "*Viable*" iniciando de esta manera su implementación acorde con las fechas mencionadas.

3.2. Herramientas a usar.

3.2.1. Software.

Para el desarrollo de software de este prototipo, es necesario hacer mención de algunas de las siguientes herramientas, para tener una idea clara sobre qué herramientas estamos utilizando y porque es que las estamos utilizando:

HTML5. HTML comenzó mucho tiempo atrás con una simple versión propuesta para crear la estructura básica de páginas web, organizar su contenido y compartir información, todo esto tenía la intención de comunicar información por medio de texto. El limitado objetivo de html motivó a varias

compañías a desarrollar nuevos lenguajes y programas para agregar características a la web nunca antes implementadas.

Dos de las opciones propuestas fueron Java y Flash; ambas fueron muy aceptadas y consideradas como el objetivo de la internet, sin embargo, con el crecimiento exponencial del internet, éste dejó de ser únicamente para los aficionados de los computadores y pasó a ser usado como un campo estratégico para los negocios y para la interacción social, ciertas limitaciones presentes en ambas tecnologías probaron ser una sentencia de muerte. Esta falta de integración resultó ser crítica y preparó el camino para la evaluación de un lenguaje del cual hablaremos un poco más a detalle después: JavaScript. Sin embargo, pese a su gran impacto, el mercado no terminó de adoptarlo plenamente y rápidamente su popularidad fue declinando, y el mercado terminó enfocando su atención a Flash. No fue hasta que los navegadores mejoraron su intérprete para JavaScript y la gente se empezaba a dar cuenta de las limitaciones que ofrecía Flash, que JavaScript fue implementado y comenzó a innovar la forma en la que se programaba la web. Al cabo de unos años, JavaScript, html y css eran considerados como la más perfecta combinación para evolucionar la Web.

HTML5 es una mejora de esta combinación, lo que unió todos estos elementos. HTML5 propone estándares para cada aspecto de la Web y también un propósito claro para cada una de las tecnologías involucradas. A partir de esto, html provee los elementos estructurales, CSS se concentra en volver esta estructura utilizable y atractiva a la vista, y JavaScript tiene todo lo necesario para brindar dinamismo y construir aplicaciones web completamente funcionales. Cabe mencionar que HTML5 funciona diferente dependiendo del navegador y la versión en la que se esté trabajando, algunos soportan más características o diferentes funcionalidades que otros.

CSS3.

Ya se ha mencionado anteriormente como es que HTML5 fue evolucionando a un grado de combinación de estructura y diseño, sin embargo, la web demanda diseño y funcionalidad, no solamente organización estructural o definición de secciones, la función de CSS se concentra en volver la estructura de HTML utilizable y atractivo a la vista.

Oficialmente CSS no tiene nada que ver con HTML4, no es parte de la especificación, es de hecho, un complemento desarrollado para superar las limitaciones y reducir la complejidad de HTML. Al principio, atributos den-

tro de las etiquetas HTML proveían estilos esenciales para cada elemento, pero a medida que HTML evolucionó, la escritura de códigos se volvió más compleja y html por sí mismo no pudo satisfacer más las demandas de los diseñadores. En consecuencia a esta demanda, CSS fue adoptado como la forma de separar la estructura de la presentación, y ha ido creciendo y ganando importancia, pero siempre desarrollado en paralelo enfocado en las necesidades de los diseñadores y apartado de la estructura de HTML.

La versión 3 de CSS sigue el mismo camino, pero esta vez con un mayor compromiso. La especificación de HTML5 fue desarrollada considerando CSS a cargo del diseño, Debido a esta consideración, la integración entre HTML y CSS es ahora vital para el desarrollo web y esta razón por la que cada vez que mencionamos HTML5 también estamos haciendo referencia a CSS3, aunque oficialmente se trate de dos tecnologías completamente separadas. Las nuevas características incorporadas en CSS3 están siendo implementadas e incluidas junto al resto de la especificación en navegadores compatibles con HTML5 [9].

JavaScript.

JavaScript es considerado como el lenguaje de programación de html y de la web. Es un lenguaje de programación fácil de usar y muy versátil para el ámbito de la comunicación en redes. Los programas, llamados "scripts", se ejecutan en el navegador (Mozilla, Google Chrome, Internet Explorer, etc.) normalmente consisten en unas funciones que son llamadas desde el propio html cuando algún evento sucede.

Su primera aproximación a un uso real, fue en mayor parte para "dar vida a una página web", como dar animaciones a un botón, interacciones en tiempo real, entre otras más. JavaScript fue desarrollado por Netcape, a partir del lenguaje Java, que en ese momento tenía mucho auge y popularidad, y su principal diferencia es que JavaScript sólo "funciona" dentro de una página html.

JavaScript fue declarado como estándar del European Computer Manufacturers Association (ECMA) en 1997, y poco después, también fue estandarizado por ISO [20].

JavaScript es un lenguaje interpretado, usado mayormente como complemento de ciertos objetivos específicos, sin embargo, uno de las innovaciones que ayudó a JavaScript fue el desarrollo de nuevos motores de interpretación, creados para acelerar el procesamiento del código. La clave de los motores más exitosos fue transformar el código de Javascript en código máquina para

obtener una velocidad de ejecución mejor que antes. Esto a la vez permitió superar viejas limitaciones de rendimiento y confirmar el lenguaje JavaScript como la mejor opción para la Web.

Para aprovechar esta prometedora plataforma de trabajo ofrecida por los nuevos navegadores, JavaScript fue expandido en cuestión de portabilidad e integración, a la vez, interfaces de programación de aplicaciones (APIs) fueron incorporando por defecto con cada navegador para asistir a JavaScript en funciones elementales. El objetivo de esto, fue principalmente hacer disponible poderosas funciones a través de técnicas de programación sencillas y estándares, expandiendo el alcance del lenguaje y facilitando la creación de programas útiles para la Web [9].

CryptoJs.

CryptoJs es una colección estándar y segura de algoritmos criptográficos implementados para JavaScript usando las mejores prácticas y patrones. Es rápida y tiene una interfaz consistente y simple. Cuenta con algoritmos tales como: Hasher Algorithms (SHA-1, SHA-2), Cipher Algorithms (DES, AES), Block Modes and Padding, por mencionar algunos [11]. El objetivo de usar esta herramienta es usar los métodos ya implementados en *CryptoJs* para la generación de código hash para una mejor y rápida ejecución del sistema.

Función Hash SHA-1.

La función hash SHA-1 se emplea actualmente en diferentes aplicaciones de seguridad, una de las más populares es la comprobación de integridad de archivos. Estas comprobaciones suelen representarse en una cadena de 40 caracteres alfanuméricos, que corresponden a los 160 bits que genera dicha función hash. SHA-1 fue desarrollado por US National Security Agency (NSA)¹ y publicado por National Institute of Standards and Technology (NIST)². Esta función hash es la segunda iteración de la función hash SHA-0 [8].

El uso del algoritmo de hashing se empleará en la creación del certificado para un usuario (tomando como parámetros el nombre de usuario y su contraseña), debido a que en este prototipo aún no se cuenta con el *servidor autenticador*. El mensaje como resultado de aplicar el algoritmo hash, se

¹NSA lidera el gobierno de Estados Unidos en el área de Criptografía con el fin de obtener una ventaja de decisión para la Nación y sus aliados en todas las circunstancias.

²NIST es uno de los laboratorios de ciencias físicas más antiguos de Estados Unidos.

inyectará en el protocolo HTTP, como se ha mencionado en la descripción del prototipo II.

Wireshark.

Wireshark es una analizador de paquetes de red. Un analizador captura paquetes de red y muestra los datos del paquete con el mayor detalle posible. Ésta herramienta es software libre y es el mejor analizador de paquetes hoy en día [27]. Utilizaremos Wireshark para analizar los paquetes que viajan a través de la red, en este caso la petición modificada la cual contiene el certificado y el patrón ocultados mediante el método *Chaffing*.

3.2.2. Hardware.

En el ámbito del hardware, utilizaremos los equipos de cómputo con los cuales contamos actualmente los integrantes de este equipo, los cuales se especificarán a continuación:

Equipo de hardware utilizado. [1]	
Marca	Asus
Modelo	X550VC
Procesador	Intel Core i5
Tarjeta de video	NVidia GForce 720
Memoria RAM	12 GB
Disco duro	1TB

Equipo de hardware utilizado. [2]	
Marca	HP
Modelo	Pavilion g4
Procesador	Intel Core i3
Tarjeta de video	Intel Sandybridge Mobile
Memoria RAM	6 GB
Disco duro	500GB

Equipo de hardware utilizado. [3]	
Marca	DELL
Modelo	Inspiron 5567
Procesador	Intel Core i7
Tarjeta de video	Radeon (TM) R7 M445
Memoria RAM	16 GB
Disco duro	1TB

Equipo de hardware utilizado. [4]	
Marca	HP
Modelo	Pavilion 15-p000ns
Procesador	AMD A A8-5545M
Tarjeta de video	Radeon R8 M540
Memoria RAM	8 GB
Disco duro	1TB

3.3. Arquitectura del sistema.

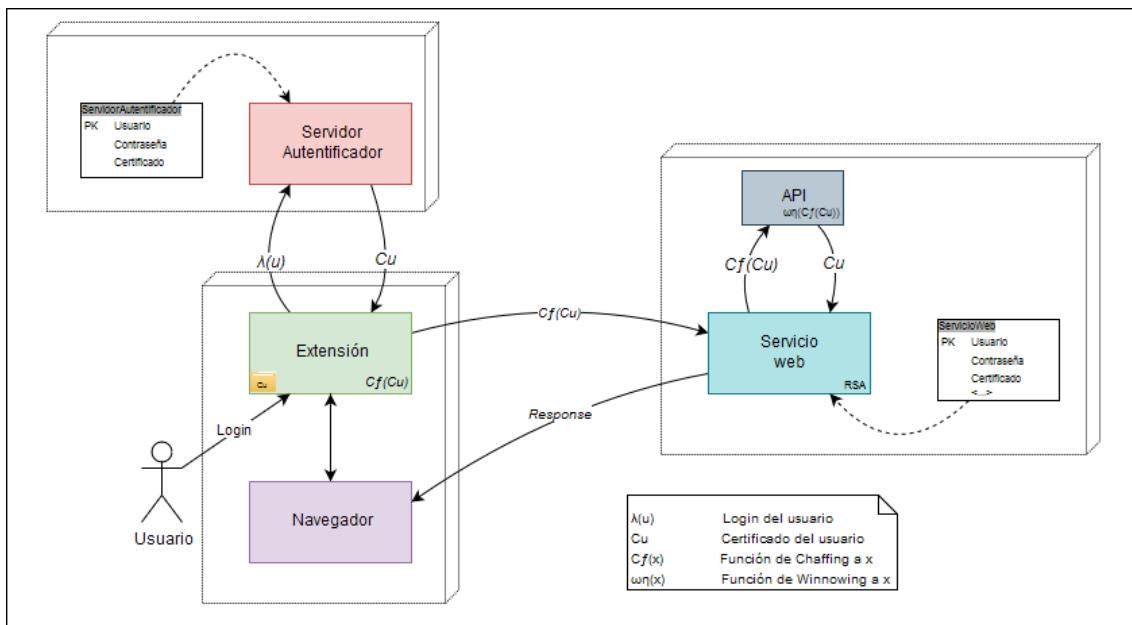


Figura 3.1: Arquitectura General del Sistema

3.3.1. Descripción de la arquitectura del sistema.

El sistema se compone de 3 grandes bloques los cuales se comunicarán vía red:

1. **Navegador Chrome con la Extensión instalada:** Este primer bloque es el que se encuentra interactuando directamente con el usuario de nuestro sistema, consiste en la extensión creada por nosotros y el navegador en el que el usuario realiza peticiones a diferentes servicios en la web.
2. **Servidor autentificador:** Este bloque va ser el encargado de generar los certificados para cada usuario que se registre en la extensión y enviarlos a la extensión. Para la generación de dichos certificados utilizaremos una autoridad certificadora con lo que garantizamos la seguridad de estos mismos. Por otro lado para almacenar los datos de nuestros usuarios contaremos con una tabla que contenga como principales campos:
 - Usuario
 - Contraseña
 - Certificado
3. **Servidor web con API instalada:** En este módulo el servicio web contará con una API, que se encargará de reconocer las peticiones que se reciban con nuestro método de autenticación y será la encargada de interpretar los datos y facilitarle la información de autenticación al servicio. Es importante destacar que el servicio almacenará el certificado en cuestión para que el usuario pueda autenticarse la próxima vez de forma automática.

Es importante mencionar que la comunicación entre cada uno de los bloques se realizará mediante técnicas que permitan la confidencialidad de los datos, por un lado la comunicación del certificado que viajará entre la extensión y el servicio web se encontrará oculto mediante Chaffing and Winnowing y el patrón necesario para el método se encontrará cifrado mediante RSA. La comunicación entre el Servidor autentificador y la Extensión se encontrará oculto mediante un socket seguro.

3.4. Diagrama de casos de uso general.

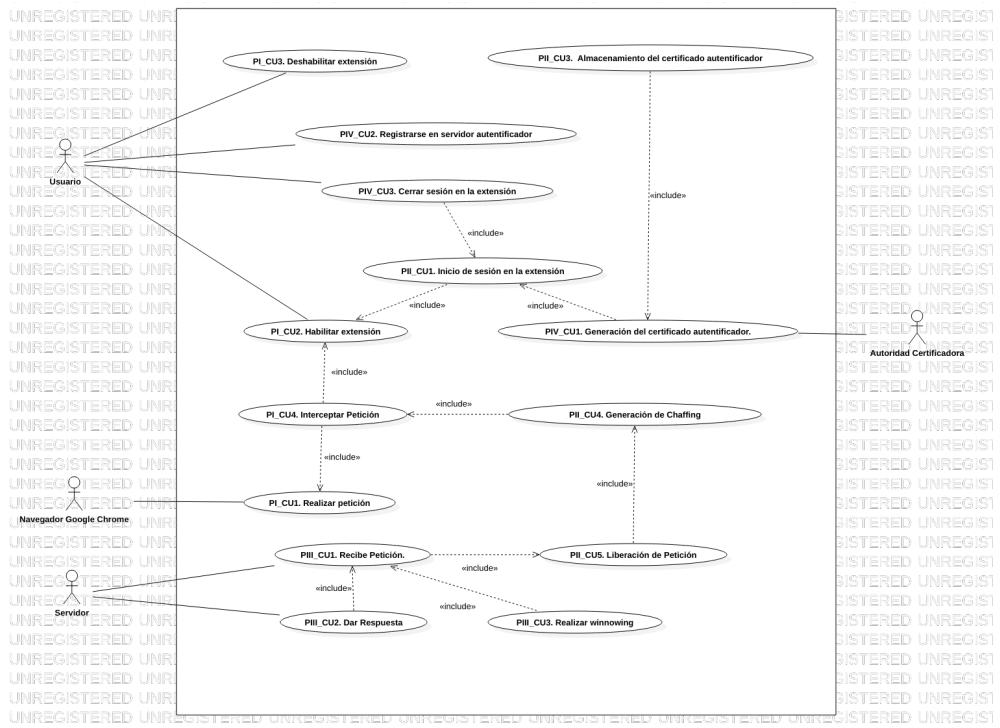


Figura 3.2: Diagrama de casos de uso general del sistema

NOTA: En la sección diseño, cada prototipo describirá sus casos de uso correspondientes para su funcionamiento.

3.5. Componente I. Extensión.

3.5.1. Descripción.

Este prototipo permite a la extensión poder interceptar peticiones hechas por el usuario a través del navegador de Google Chrome, una vez que se intercepta la petición, ésta podrá ser modificada. La modificación se hará sólo mientras la extensión esté habilitada, y tiene como objetivo injectar el certificado autenticador en el encabezado del protocolo. Este certificado será simulado (sólo para este prototipo) por la misma extensión a partir de los datos del inicio de sesión. Para la creación de dicho certificado, se usará el algoritmo de hashing SHA-1, tomando como argumentos de entrada usuario

y contraseña, generando así, una cadena resultante de 160 bits, sin embargo, para los siguientes prototipos, se manejará una autoridad certificadora la cual recibirá los datos del inicio de sesión para que genere el certificado del usuario. Una vez que dicho certificado es inyectado, la extensión deberá liberar la petición para que salga a red.

El propósito de este prototipo es utilizar la técnica de *Chaffing and Winnowing* en este nuevo método de autenticación, para evitarle al usuario la tediosa tarea de ingresar sus credenciales cada vez que accede al servicio y brindarle la seguridad necesaria al iniciar de sesión.

Para inyectar el certificado autentificador, es necesario crear un "*patrón de chaffing*", este patrón lo generaremos aleatoriamente para después mandarlo junto con la petición HTTP. Por el momento, dicho patrón no irá cifrado, ya que para esto es necesario la implementación del servidor del servicio web de prueba, para poder conocer su llave pública y cifrar el patrón. Sin embargo, en el prototipo 1 del subsistema 3 se implementará el servidor y con ello su cifrado asimétrico. El objetivo de mandar el patrón junto con el protocolo HTTP, es que el servidor pueda leer el patrón y realizar la etapa de *winnowing*, para extraer el certificado.

3.5.2. Estudio de requerimientos.

3.5.2.1. Requerimientos Funcionales.

CI_RF1. Interceptar petición HTTP. La extensión deberá interceptar la petición HTTP del navegador, en cuanto el usuario realice alguna a través de éste.

CI_RF2. Deshabilitar extensión. El usuario podrá deshabilitar la extensión, para que ésta no vigile su actividad en el navegador.

CI_RF3. Habilitar extensión. El usuario podrá habilitar la extensión, para que ésta vigile las peticiones HTTP.

CI_RF4. Validar petición. La extensión deberá analizar la petición previamente recibida, y validar si ésta es HTTP(S) o no.

CI_RF5. Bloquear salida de petición. La extensión deberá evitar que la petición salga a red, deteniéndola para aplicar la etapa de *Chaffing*.

CI_RF6. Inicio de sesión en la extensión. La extensión contará con una interfaz para el ingreso de datos del usuario, donde ingresará un usuario y contraseña.

CI_RF7. Generación del certificado autentificador. Para este prototipo, la generación del certificado autentificador se hará del lado del cliente, simulando la tarea de una entidad certificadora, permitiendo así generar automáticamente esta llave la cual servirá para el proceso de *chaffing* del mensaje en el protocolo HTTP.

CI_RF8. Almacenamiento del certificado autentificador. La extensión deberá almacenar el certificado autentificador.

CI_RF9. Generación de patrón de Chaffing. La extensión generará un patrón para poder implementar el método de *Chaffing*. Este patrón será generado al azar, y es aquel que se usará para introducir el código autentificador en el protocolo HTTP.

CI_RF10. Etapa de Chaffing. Por medio del método *Chaffing* se crearán paquetes para agregar al encabezado HTTP que se ha interceptado gracias al requerimiento funcional CI_RF1. Interceptar petición HTTP, utilizando el patrón de *Chaffing* del requerimiento funcional CI_RF9. Generación de patrón de *Chaffing*

CI_RF11. Liberación de Petición. Se liberará el bloqueo a la petición HTTP impuesto por el requerimiento funcional CI_RF5. Bloquear salida de petición.

3.5.2.2. Requerimientos no Funcionales.

CI_RNF1. Plataforma de implementación. La extensión será implementada en el navegador Google Chrome Desktop.

CI_RNF2. Versión del navegador La extensión funcionará a partir de la versión 28.0.

CI_RNF3. Tecnologías para la interfaz de usuario Para el sistema se hará uso de HTML5, JavaScript, CSS3, JSON.

CI_RNF4. Permitir ejecución de JavaScript en Google Chrome.

Para el correcto funcionamiento de la extensión, es necesario que se permita la ejecución de javascript en el navegador Google Chrome.

CI_RNF5. Conexión a internet. Para el funcionamiento de la extensión, no es necesario que se tenga conexión a internet.

CI_RNF6. Tamaño del código autentificador. El tamaño del código autentificador es de 160 bits. Para este prototipo se hará uso de la función *hash* tomando como argumentos el nombre de usuario y contraseña del usuario que se desea generar el código de hash.

CI_RNF7. Almacenado de archivo en la extensión. Se necesita tener almacenado el archivo en la extensión de Google Chrome. Específicamente, utilizamos el **Storage** para almacenarlo.

CI_RNF8. Conexión a internet. Para el funcionamiento de este prototipo, es necesario tener acceso a internet.

3.5.3. Reglas del negocio.

CI_RN1. Extensión habilitada. En cuanto el usuario lo indique por medio de la Interfaz de Usuario, la extensión deberá vigilar la actividad que éste realice en el navegador para interceptar una petición.

CI_RN2. Extensión deshabilitada. En cuanto el usuario lo indique por medio de la Interfaz de Usuario, la extensión dejará de vigilar la actividad que éste realice en el navegador.

CI_RN3. Petición válida. La extensión modificará la petición siempre y cuando se trate de una petición válida HTTP .

CI_RN4. Inicio de sesión de extensión por usuario. Cada usuario que desee utilizar la extensión sólo deberá tener una cuenta con un usuario y una contraseña respectiva a este usuario.

CI_RN5. Acceso a internet. Se debe de contar con acceso a internet para que la extensión pueda enviar al servidor la petición modificada.

CI_RN6. Longitud de código autentificador. La longitud del código autentificador es de 40 caracteres, debido a que la función de SHA-1 es un

algoritmo de codificación de 160 bits que genera un hash hexadecimal de 40 caracteres.

CI_RN7. Longitud del campo de usuario. La longitud del usuario no debe pasar de 20 caracteres, y mínimo será de 3 caracteres.

CI_RN8. Longitud del campo contraseña. La longitud de la contraseña no debe pasar de 16 caracteres, y mínimo sera de 8 caracteres.

CI_RN9. Caracteres permitidos en campo usuario. Los caracteres permitidos en el campo de usuario son únicamente símbolos alfanúmericos y guion bajo.

CI_RN10. Caracteres permitidos en campo contraseña. Los caracteres permitidos en el campo de contraseña son únicamente símbolos alfanúmericos así como los símbolos - @ / # ? .

CI_RN11. Formato de contraseña. La contraseña debe tener al menos un número y una letra mayúscula.

3.6. Componente II: Servidor autenticador.

3.6.1. Descripción.

Para este componente, vamos a implementar un servidor autenticador en el cual se crearán y almacenarán los certificados de los usuarios en una base de datos. En este servicio, los usuarios tendrán registrada una cuenta a la cual accederán desde la extensión del componente 1. Una vez que inicien sesión en la extensión, este servidor autenticador regresará como respuesta el certificado generado para que la extensión lo almacene. Para la creación del certificado autenticador se utilizará la herramienta OpenSSL, además, la comunicación entre extensión y servidor se hará bajo SSL/TLS.

La principal función de este componente es gestionar las cuentas y certificados en una base de datos, de tal forma que el componente 1 (extensión de Google Chrome) se pueda comunicar con este componente ya sea para que le genere un certificado a una cuenta (en el caso de que el usuario se esté registrando en el servidor autenticador por primera vez) o para mandarle su certificado si es que ya se encuentra registrado en el servidor.

El propósito de este componente es poder crear y utilizar un certificado real, generado por una autoridad certificadora de confianza y con el cual se pueda autenticar a un usuario en un servicio web. Como sabemos, el certificado emitido por la autoridad certificadora es de tipo público por lo que puede ser visible para cualquier entidad.

3.6.2. Estudio de requerimientos.

3.6.2.1. Requerimientos funcionales.

CII_RF1. Creación de nuevo usuario. La autoridad certificadora podrá crear una nueva instancia en la base de datos de acuerdo a los datos recuperados por la extensión (Usuario y contraseña), si es que estos no se encuentran guardados en la base de datos.

CII_RF2. Generar certificado. La autoridad certificadora deberá generar un certificado diferente para cada usuario que se registre en la extensión con los datos proporcionados por la misma.

CII_RF3. Asignar certificado. La autoridad certificadora deberá asignar el certificado generado al usuario correspondiente en la base de datos.

CII_RF4. Devolver certificado. La autoridad certificadora deberá enviar el certificado correspondiente al usuario quien realiza la solicitud para obtener el certificado.

CII_RF5. Actualizar certificado. La autoridad certificadora deberá actualizar el certificado cuanto éste haya caducado.

3.6.2.2. Requerimientos no funcionales.

CII_RNF1. Plataforma de implementación. La autoridad certificadora será implementada en NodeJs.

CII_RNF2. Version de SSL/TLS. La autoridad certificadora usará como conexión, así como la generación de certificado, OpenSSL con la versión 1.1.1.

CII_RNF3. Base de datos. La autoridad certificadora se conectará a una base de datos MongoDB 4.0.10.

3.6.3. Reglas del negocio.

CII_RN1. Acceso a internet. Se debe de contar con acceso a internet para que la autoridad certificadora pueda enviar a la extensión el certificado generado.

CII_RN2. Conexión a la base de datos. La autoridad certificadora cuenta con un pull de conexiones a la base de datos para poder insertar u obtener certificados de los usuarios.

CII_RN3. Conexión SSL. La autoridad certificadora tiene una conexión SSL con la extensión para poder así enviar el certificado de manera segura y cifrada.

3.7. Componente III: Servicio Web y API.

3.7.1. Descripción.

Para el componente III, se va a implementar un servicio web de prueba para realizar la etapa de *winnowing* a la petición HTTP que reciba de la extensión. Esto implica la modificación del servidor de prueba implementado en Apache para que detecte este tipo de autentificación y la creación de un algoritmo que realice el procesos de *winnowing* al protocolo. Así mismo, el servicio web implementará un cifrado asimétrico (RSA), esto con la finalidad de que el componente I pueda tomar la llave pública del servidor y cifrar el "*patrón de chaffing*" que se mandará en la petición. Este servidor web tendrá una API la cual se encargará de realizar el proceso de *winnowing*, descifrando lo que reciba del componente I con la llave privada del servidor.

El propósito de este componente es poder obtener el certificado que identificará a cada usuario, para poder validarla y saber si se debe de dar acceso o negar el mismo. Cabe mencionar que, la primera vez que el servidor reciba el certificado autenticador en cada servicio, pedirá al usuario que se inicie sesión con la finalidad de poder asociar este certificado a una cuenta de un servicio; para las peticiones posteriores, el certificado ya contará con una

cuenta asociada a la cual podrá dar acceso siempre y cuando las credenciales sean correctas.

3.7.2. Estudio de requerimientos.

3.7.2.1. Requerimientos funcionales.

CIII_RF1. Guardar certificados. Si el servidor no tiene asociado el certificado que se recibe del componente I en la base de datos, éste lo guardará asociandolo con un inicio de sesión.

CIII_RF2. Comunicación con autoridad certificadora. El servidor autentificador podrá tener comunicación con una autoridad certificadora para el intercambio de información.

CIII_RF3. Obtención de certificado autentificador. Una vez realizada la comunicación con la autoridad certificadora, obtendremos un certificado autentificador que identificará a un usuario.

CIII_RF4. Generación de llaves. El servidor web puede generar un par de llaves (pública y privada) para su uso en cifrados asimétricos (en este caso, RSA).

3.7.2.2. Requerimientos no funcionales.

CIII_RNF1. Plataforma de implementación. Las pruebas del servidor web serán realizadas en el servidor Apache2.

CIII_RNF2. Base de datos. Se utilizará una base de datos en MySQL para guardar la información de los usuarios.

CIII_RNF3. Tamaño de llaves. Se utilizarán llaves de un tamaño de 2048 bits para el cifrado de tipo RSA.

3.7.2.3. Reglas del negocio.

CIII_RN1. Conexión a internet. Se debe de contar con una conexión estable a internet para evitar perder paquetes en todo el proceso.

CIII_RN2. Conexión a base de datos. El servidor debe tener una correcta conexión a la base de datos para su correcto funcionamiento.

CIII_RN3. API en el servidor. El servidor debe de contar con la API para que pueda realizar el procesos de *winnowing*.

Capítulo 4

Diseño.

4.1. Componente I.

4.1.1. Diagrama de casos de uso

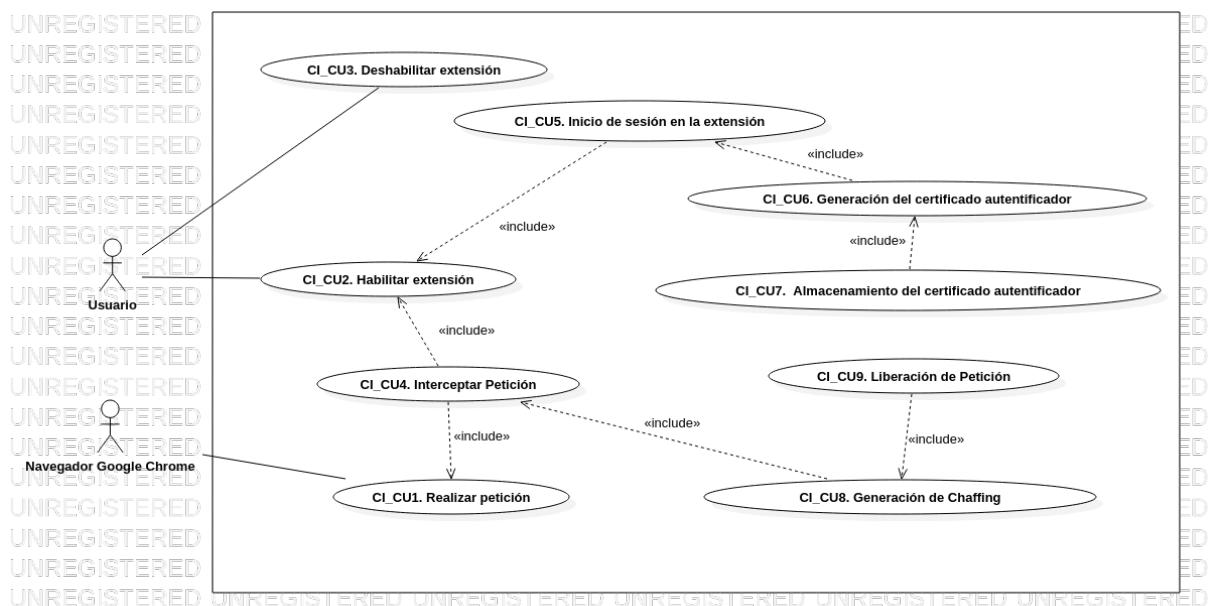


Figura 4.1: Diagrama de casos de uso del Componente I.

4.1.2. Descripción de casos de uso.

Caso de uso: CI_CU1. Realizar petición.	
Concepto	Descripción
Actor	Navegador de Google Chrome.
Propósito	Este caso de uso permite al navegador realizar una petición HTTP, ordenada por el usuario o un sistema externo.
Entradas	URL del servicio web solicitado.
Salidas	Petición HTTP.
Pre-condiciones	Algún agente externo (Sistema o usuario) ha ordenado al navegador mandar una petición HTTP.
Post-condiciones	Creación de la petición HTTP.
Reglas del negocio	-
Errores	La petición no se pudo realizar. La petición no es tipo HTTP.

Cuadro 4.1: Descripción CU: CI_CU1

... Trayectoria Principal ...

1. ***El Usuario o El Sistema Externo*** realiza una petición HTTP en el navegador Google Chrome.
2. ***El navegador*** realiza la petición.

... Fin de la Trayectoria Principal ...

... Trayectoria Alternativa 1 ...

1. ***El Usuario o El Sistema Externo*** realiza una petición que no es HTTP en el navegador Google Chrome.
2. ***El navegador*** realiza la petición.

Caso de uso: CI_CU2. Habilitar extensión.	
Concepto	Descripción
Actor	Usuario.
Propósito	Este caso de uso, permite al usuario habilitar la extensión, para que ésta sea capaz de ver todas las peticiones que realiza el navegador.
Entradas	Indicación de habilitar extensión, mediante interfaz de usuario.
Salidas	-
Pre-condiciones	CI_CU3.
Post-condiciones	-
Reglas del negocio	CI_RN1.
Errores	No se puede habilitar la extensión.

Cuadro 4.2: Descripción CU: CI_CU2

... Fin de la Trayectoria Alternativa 1 ...

... Trayectoria Principal ...

1. **El usuario** da click en el ícono de la extensión .

2. **El usuario** da click en el botón .

3. **La extensión** empieza a vigilar las peticiones que se realicen a través del navegador.

... Fin de la Trayectoria Principal ...

... Trayectoria Alternativa 1 ...

1. **La extensión** no muestra el botón 

Caso de uso: CI_CU3. Deshabilitar extensión.	
Concepto	Descripción
Actor	Usuario.
Propósito	Este caso de uso permite al usuario deshabilitar la extensión, para que ésta ignore todas las peticiones que se realicen por medio del navegador.
Entradas	Indicación de deshabilitar extensión, mediante interfaz de usuario.
Salidas	-
Pre-condiciones	CI_CU2.
Post-condiciones	-
Reglas del negocio	CI_RN2.
Errores	No se puede deshabilitar la extensión.

Cuadro 4.3: Descripción CU: CI_CU3

... Fin de la Trayectoria Alternativa 1 ...

... Trayectoria Principal ...

1. **El usuario** da click en el ícono de la extensión .
2. **El usuario** da click en el botón **Desactivar**.
3. **La extensión** deja de vigilar las peticiones que se realicen a través del navegador.

... Fin de la Trayectoria Principal ...

... Trayectoria Alternativa 1 ...

1. **La extensión** no muestra el botón **Desactivar**, por ende el usuario no puede dar click.

Caso de uso: CI_CU4. Interceptar petición.	
Concepto	Descripción
Actor	-.
Propósito	Este caso de uso interceptará las peticiones HTTP que el navegador realice para su análisis.
Entradas	Petición realizada por el navegador
Salidas	-
Pre-condiciones	CI_CU1. CI_CU2.
Post-condiciones	-
Reglas del negocio	CI_RN1. CI_RN3.
Errores	La petición no se genera correctamente.

Cuadro 4.4: Descripción CU: CI_CU4

... Fin de la Trayectoria Alternativa 1 ...

... Trayectoria Principal ...

1. *El usuario* ingresa una URL en el navegador.
2. *El navegador* genera una petición HTTP.
3. *La extensión* Intercepta la petición realizada por el navegador para su análisis

Caso de uso: CI_CU5. Inicio de sesión en la extensión	
Concepto	Descripción
Actor	Usuario
Propósito	<p>Este caso de uso permite al usuario poder iniciar sesión en la extensión para posteriormente obtener un código autentificador, basado en esos datos, al cual se le aplicará <i>Chaffing</i>.</p> <p>Sólo se requerirá iniciar sesión una sola vez, ya que después, sólo es necesario CIR el código generado para autenticarse en el servicio web.</p>
Entradas	Usuario y Contraseña
Salidas	Código autentificador el cual hace referencia al usuario iniciado
Pre-condiciones	Haber instalado la extensión en el navegador Google Chrome y habiéndola habilitado.
Post-condiciones	Con los datos introducidos por el usuario, se obtendrá el código autentificador del mismo, para que lo guarde en su dispositivo y lo pueda usar después.
Reglas del negocio	CI_RN1. CI_RN4. CI_RN7. CI_RN8. CI_RN9. CI_RN10. CI_RN11.
Errores	No se encuentra usuario registrado No se puede obtener el código autentificador No se pudo guardar el código autentificador Contraseña no válida

Cuadro 4.5: Descripción CU: CI_CU5

... Fin de la Trayectoria Principal ...

... Trayectoria Principal ...

1. **El Usuario** realiza un inicio de sesión por primera vez en la extensión.
2. **La extensión** obtendrá los parámetros de usuario y contraseña para generar un código autentificador único.

... Fin de la Trayectoria Principal ...

... Trayectoria Alternativa 1 ...

1. *El Usuario* ingresa usuario y/o contraseña no validos.
2. *La extensión* no podrá obtener los datos del usuario.

... Fin de la Trayectoria Alternativa 1 ...

Caso de uso: CI_CU6. Generación del certificado autentificador.

Concepto	Descripción
Actor	-
Propósito	Este caso de uso generará un certificado para el usuario, basados en los datos que ingrese en la extensión (usuario y contraseña).
Entradas	Usuario y contraseña ingresados en la extensión.
Salidas	Certificado autentificador del usuario.
Pre-condiciones	Contar con la extensión habilitada. e ingresar un usuario y contraseña
Post-condiciones	-
Reglas del negocio	CLRN7. CLRN8. CLRN9. CLRN10. CLRN11.
Errores	Error al generar el certificado.

Cuadro 4.6: Descripción CU: CI_CU6

... Trayectoria Principal ...

1. *La extensión* generará un código autentificador basado en los datos ingresados por el usuario.

... Fin de la Trayectoria Principal ...

... Trayectoria Alternativa 1 ...

1. *La extensión* no puede generar el código autentificador.
2. *La extensión* mostrará al usuario un mensaje de dicho error.

... Fin de la Trayectoria Alternativa 1 ...

Caso de uso: CI_CU7. Almacenamiento del certificado autentificador.

Concepto	Descripción
Actor	-
Propósito	<p>Este caso de uso permite que la extensión guarde el certificado autentificador, para que el usuario no tenga que hacerlo por el mismo. De esta manera, la extensión tendrá acceso al certificado cada que éste sea requerido.</p> <p>El lugar donde se guarda dicho certificado es en "Google Chrome Storage", una zona de memoria que Google Chrome nos brinda al desarrollar una extensión para el navegador.</p>
Entradas	Certificado autentificador.
Salidas	-
Pre-condiciones	CI_CU6..
Post-condiciones	-
Reglas del negocio	CI_RN6.
Errores	No se puede almacenar el certificado autentificador.

Cuadro 4.7: Descripción CU: CI_CU7

... Trayectoria Principal ...

1. ***La extensión*** ha creado el certificado autentificador.
2. ***La extensión*** guarda el certificado en storage.
3. ***La extensión*** muestra al usuario el siguiente mensaje "Certificado guardado en Storage" en la figura 4.17

... Fin de la Trayectoria Principal ...

... Trayectoria Alternativa 1 ...

1. ***La extensión*** no ha creado el certificado autentificador.
2. ***La extensión*** no guarda el certificado autentificador en storage.
3. ***La extensión*** muestra al usuario el siguiente mensaje "Certificado no encontrado" en la figura 4.18

... Fin de la Trayectoria Alternativa 1 ...

... Trayectoria Alternativa 2 ...

1. ***La extensión*** ha creado el certificado autentificador.
2. ***La extensión*** no puede guardar el certificado autentificador en storage.
3. ***La extensión*** muestra al usuario el siguiente mensaje "No se pudo guardar el certificado en el Storage" en la figura 4.18

... Fin de la Trayectoria Alternativa 2 ...

Caso de uso: CI_CU8. Generación de Chaffing	
Concepto	Descripción
Actor	-
Propósito	Este caso de uso es el encargado de generar la petición modificada, es decir, de combinar el certificado con la petición HTTP mediante el método de Chaffing que decidimos aplicar.
Entradas	Certificado autentificador y Petición HTTP válida.
Salidas	Petición HTTP modificada.
Pre-condiciones	CI_CU4..
Post-condiciones	-
Reglas del negocio	CLRN3.
Errores	No se tenga una petición HTTP válida. No se cuente con un código autentificador válido.

Cuadro 4.8: Descripción CU: CI_CU8

... Trayectoria Principal ...

1. ***La extensión*** Ha recibido una petición HTTP válida.
2. ***La extensión*** Tiene un certificado guardado en storage.
3. ***La extensión*** aplica el algoritmo de Chaffing en el encabezado de la petición HTTP ocultando el certificado en los headers de ésta.
4. ***La extensión*** libera la petición modificada al servidor.

... Fin de la Trayectoria Principal ...

... Trayectoria Alternativa 1 ...

1. ***La extensión*** no ha encontrado el certificado autentificador en storage.
2. ***La extensión*** muestra al usuario el siguiente mensaje "No se encuentra certificado" en la figura 4.19

... Fin de la Trayectoria Alternativa 1 ...

... Trayectoria Alternativa 2 ...

1. ***La extensión*** no ha recibido ninguna petición HTTP válida.
2. ***La extensión*** no realiza ninguna acción ya que, aunque se cuente con el certificado al carecer de petición HTTP es imposible generar una petición modificada con Chaffing.

... Fin de la Trayectoria Alternativa 2 ...

Caso de uso: CI_CU9. Liberación de Petición.	
Concepto	Descripción
Actor	Navegador de Google Chrome
Propósito	Este caso de uso permite al Navegador de Google Chrome liberar la petición una vez que haya sido modificada por la extensión. Dentro de la petición se incluye el código autentificador junto con el patrón a utilizar en el proceso de <i>Winnowing</i> una vez que sea recibido por el servidor.
Entradas	Petición
Salidas	Petición modificada enviada en red al servidor.
Pre-condiciones	Haber completado exitosamente el proceso de <i>Chaffing</i> al igual que la creación del patrón, e injectarlo en la petición.
Post-condiciones	Con los datos generados (Código Chaffing y patrón) generados por la extensión, se deben de injectar en la petición para poder ser enviada al servidor a través de la red.
Reglas del negocio	CI_RN1 CI_RN3 CI_RN4 CI_RN5
Errores	No se cuenta con acceso a internet Hay un error de estructura en la petición

Cuadro 4.9: Descripción CU: CI_CU9

... Trayectoria Principal ...

1. **El Navegador Google Chrome** realiza una petición con el encabezado HTTP modificado, el cual contiene dentro del apartado *headers* del encabezado HTTP el certificado modificado con el proceso de *Chaffing* y el patrón que ayudará al servidor al momento de hacer el proceso de *Winnowing*.
2. **El analizador Wireshark** captura la petición generada y muestra el encabezado modificado. Esto con el fin de mostrar que se ha generado el certificado y se ha modificado exitosamente con el proceso *Chaffing*.

... Fin de la Trayectoria Principal ...

... Trayectoria Alternativa 1 ...

1. *El Navegador de Google Chrome* no puede establecer una conexión con el servidor debido a que no se cuenta con acceso a internet.
2. *El analizador Wireshark* no podrá obtener los datos del encabezado, ya que no capturará la petición.

... Fin de la Trayectoria Alternativa 1 ...

4.1.3. Diagrama de flujo (DF).

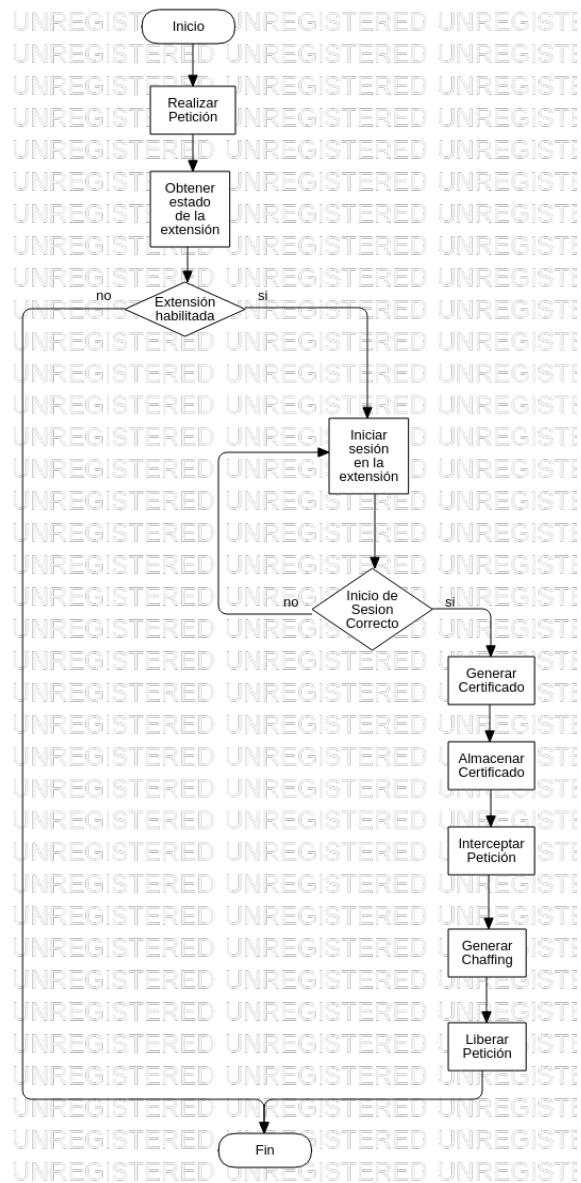


Figura 4.2: Diagrama de flujo del Componente I.

4.1.3.1. Descripción diagrama de flujo.

Para el caso de este diagrama se inicia con una petición realizada por el navegador web para luego analizar si la extensión se encuentra activada, en

caso de que no se realiza ninguna acción, pero si se encuentra se pedirá que se inicie sesión en la extensión con el propósito de generar un certificado válido para el usuario, mas tarde será necesario almacenar este certificado en la extensión y se procederá a interceptar la petición HTTP para modificarla, por lo que se genera el chaffing mediante la combinación de la petición y el certificado para luego liberar la petición modificada al servidor.

4.1.4. Diagrama de flujo de datos (DFD).

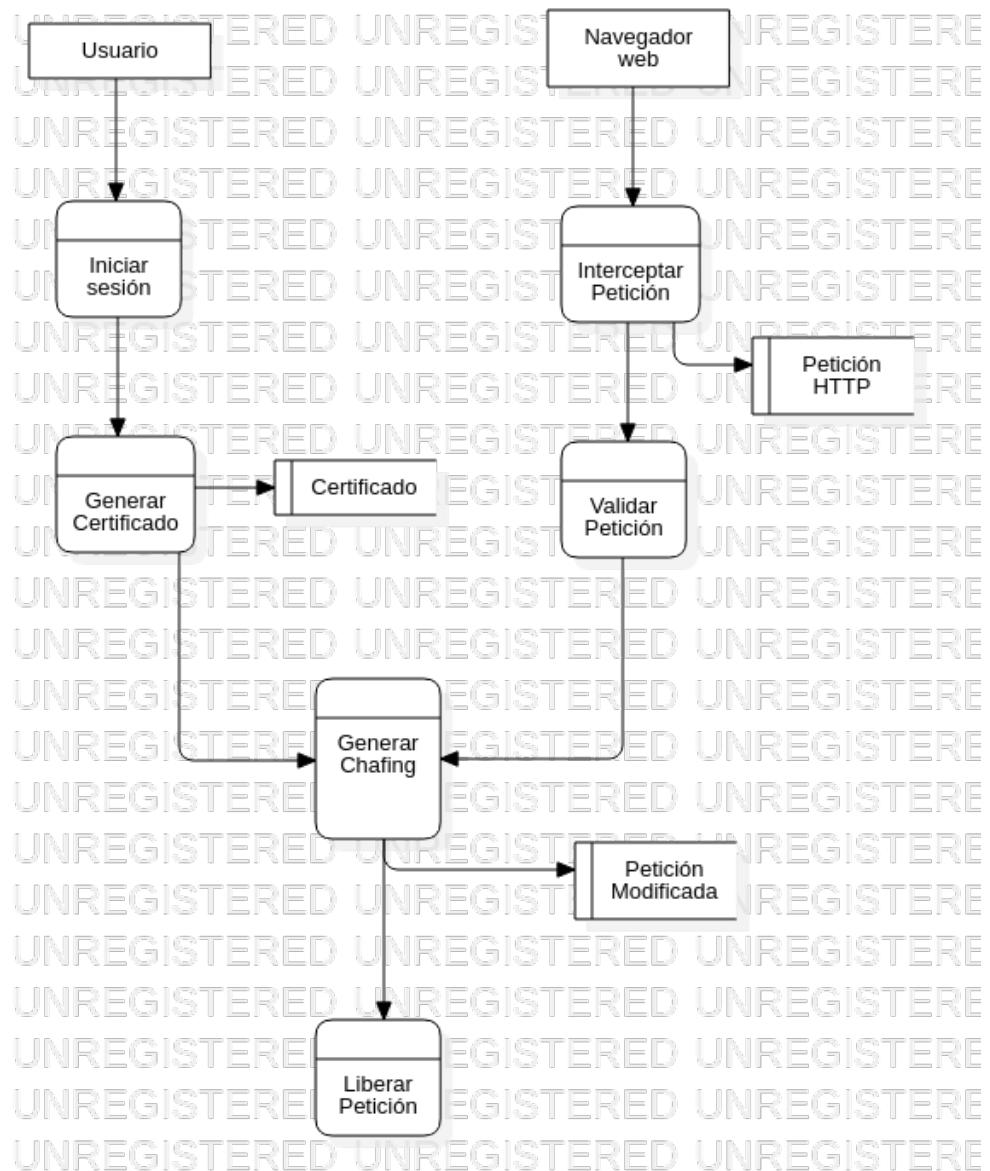


Figura 4.3: Diagrama de flujo de datos del Componente I.

4.1.4.1. Descripción diagrama de flujo de datos.

En este caso contamos con dos entidades externas, el usuario por una parte debe iniciar sesión para que se pueda generar un **Certificado** el cual

se utilizará para generar el chaffing y por otro lado el Navegador web que intercepta una **petición HTTP** que de igual manera se utilizará para generar el chaffing. Como resultado de la mezcla de estos dos se genera una **petición modificada** la cuál mas tarde se liberará para que pueda viajar hacia el servidor.

4.1.5. Diagrama de clases.

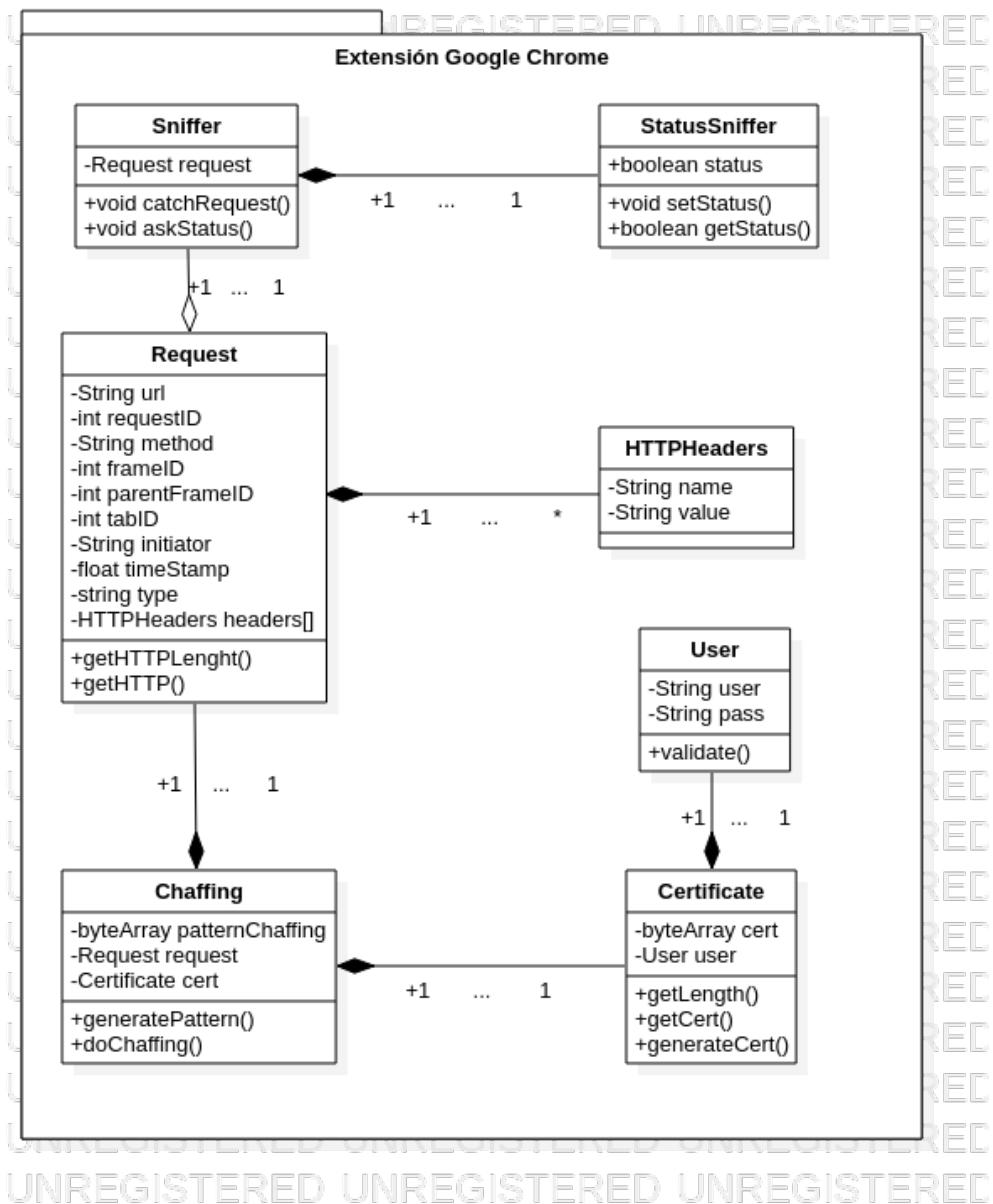


Figura 4.4: Diagrama de clases de Componente I.

4.1.5.1. Descripción de diagrama de clases

StatusSniffer

1. **status** : Variable que permite conocer y almacenar el status de la extensión (Habilitada/Deshabilitada).

- a) Tipo de dato: **boolean**.

Métodos

- a) **setStatus()**: Se establece el valor del status, True (Está activada la extensión) o False (No está activa la extensión).
 - b) **getStatus()**: Se obtiene el valor del status de la extensión, True o False.

Sniffer

1. **request** : Variable que almacena los valores de la cabecera HTTP.

- a) Tipo de dato: **Request**.

Métodos

- a) **catchRequest()**: Intercepta la petición para obtener los valores de la cabecera.
 - b) **askStatus()**: Invoca al método *getStatus()* de la clase StatusSniffer para conocer el status de la extensión.

Request

1. **url** : Variable que almacena la URL requerida.

- a) Tipo de dato: **String**.

2. **requestID** : Variable que almacena el ID de la petición.

- a) Tipo de dato: **int**.

3. **method** : Variable que almacena el tipo de método de la petición, *GET* o *POST*.

- a) Tipo de dato: **String**.

4. **frameID** : Variable que almacena el tipo del frame.

- a) Tipo de dato: **int**.
- 5. **parentFrameID** : Variable que almacena el id del frame que envía la petición.
 - a) Tipo de dato: **int**.
- 6. **tabID** : Variable que almacena el ID del tab que toma lugar en la petición.
 - a) Tipo de dato: **int**.
- 7. **initiator** : Variable que almacena el origen de la petición.
 - a) Tipo de dato: **String**.
- 8. **timeStamp** : Variable que almacena la hora cuando se dispara la petición.
 - a) Tipo de dato: **float**.
- 9. **type** : Variable que almacena el tipo de la petición.
 - a) Tipo de dato: **String**.
- 10. **headers** : Variable de tipo Array que almacena los headers a ser enviados junto con la petición.
 - a) Tipo de dato: **HTTPHeaders**.

HTTPHeaders

- 1. **name** : Variable que almacena el nombre del header a mandar junto con la petición.
 - a) Tipo de dato: **String**.
- 2. **value** : Variable que almacena el contenido del header a enviar junto con la petición.
 - a) Tipo de dato: **String**.

User

- 1. **user** : Variable que permite almacenar el valor del campo nombre de usuario.

- a) Tipo de dato: **String**.
 - b) Longitud de caracteres: **20 caracteres**.
 - c) Restricciones: La cadena sólo puede tener símbolos alfanuméricos
2. **pass** : Variable que permite almacenar el valor del campo contraseña.
- a) Tipo de dato: **String**.
 - b) Longitud de caracteres: **16 caracteres**.
 - c) Restricciones: Al menos un **número y una letra mayúscula**. La cadena sólo puede tener símbolos alfanuméricos.

Métodos

- a) **validate()** : Método que valida que los valores de las variables sean válidos.

Certificate

1. **cert** : Variable que permite almacenar el valor del certificado autenticador.
- a) Tipo de dato: **byte []**.
 - b) Longitud: **40 bytes**.
2. **user** : Variable que permite almacenar el usuario actual que se está utilizando.
- a) Tipo de dato: **User**.

Métodos:

- a) **getLength()** : método que devuelve la longitud del certificado.
- b) **getCert()** : método que devuelve el certificado.
- c) **generateCert()** : método que genera el certificado con base a los datos del usuario.

Chaffing

1. **patternChaffing** : Variable que permite almacenar el patrón de *chaffing*.
 - a) Tipo de dato: **byte** [].
 - b) Longitud: **HTTP.Length()** + **cert.Length()**.
2. **request** : Variable que permite almacenar la petición HTTP.
 - a) Tipo de dato: **Request**.
3. **cert** : Variable que permite almacenar el certificado del usuario.
 - a) Tipo de dato: **Certificate**.

Métodos:

- a) **generatePattern()** : método que genera el patrón de *chaffing*.
- b) **doChaffing()** : método que realiza el chaffing en la petición HTTP.

4.1.6. Diagramas de secuencia.

4.1.6.1. Diagrama de secuencia 1

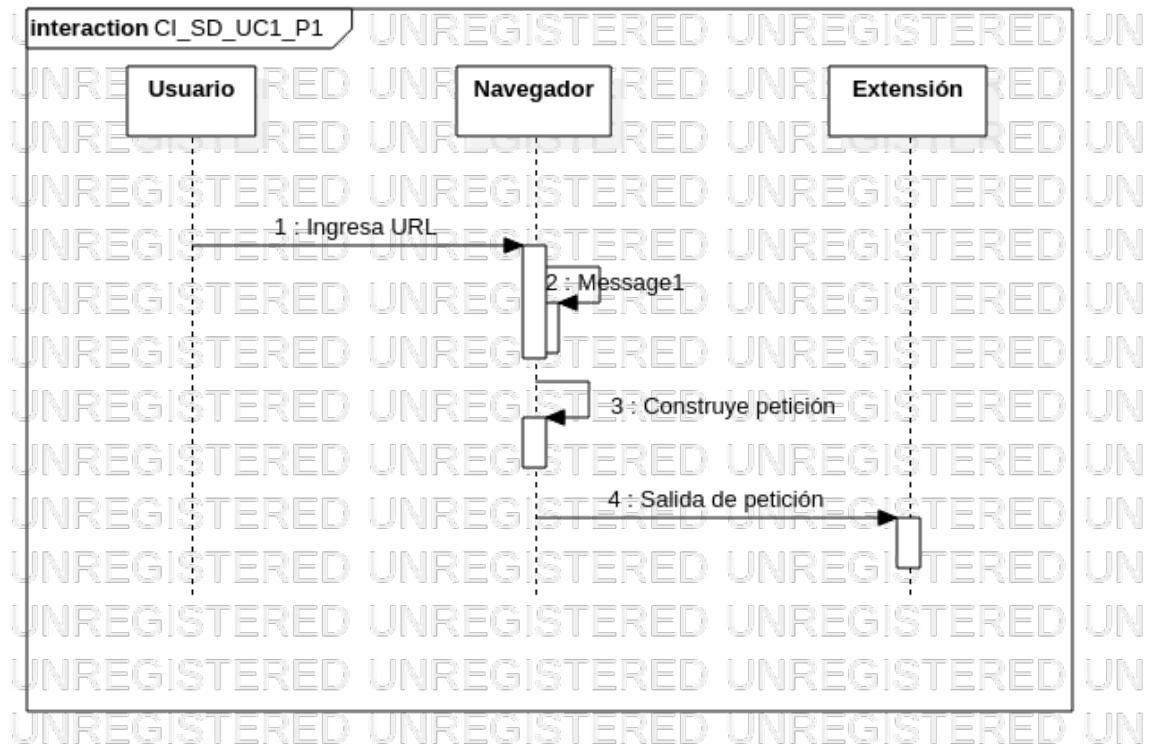


Figura 4.5: Diagrama de secuencia del CI_CU1. Realizar petición.

Descripción: Para realizar una petición, es necesario seguir la siguiente secuencia. Primeramente, el usuario ingresa un URL al navegador, para que este construya la petición que mandará. Una vez que ha construido la petición, la manda a red, pero antes de eso la extensión que actúa como un sniffer, la interceptará.

4.1.6.2. Diagrama de secuencia 2

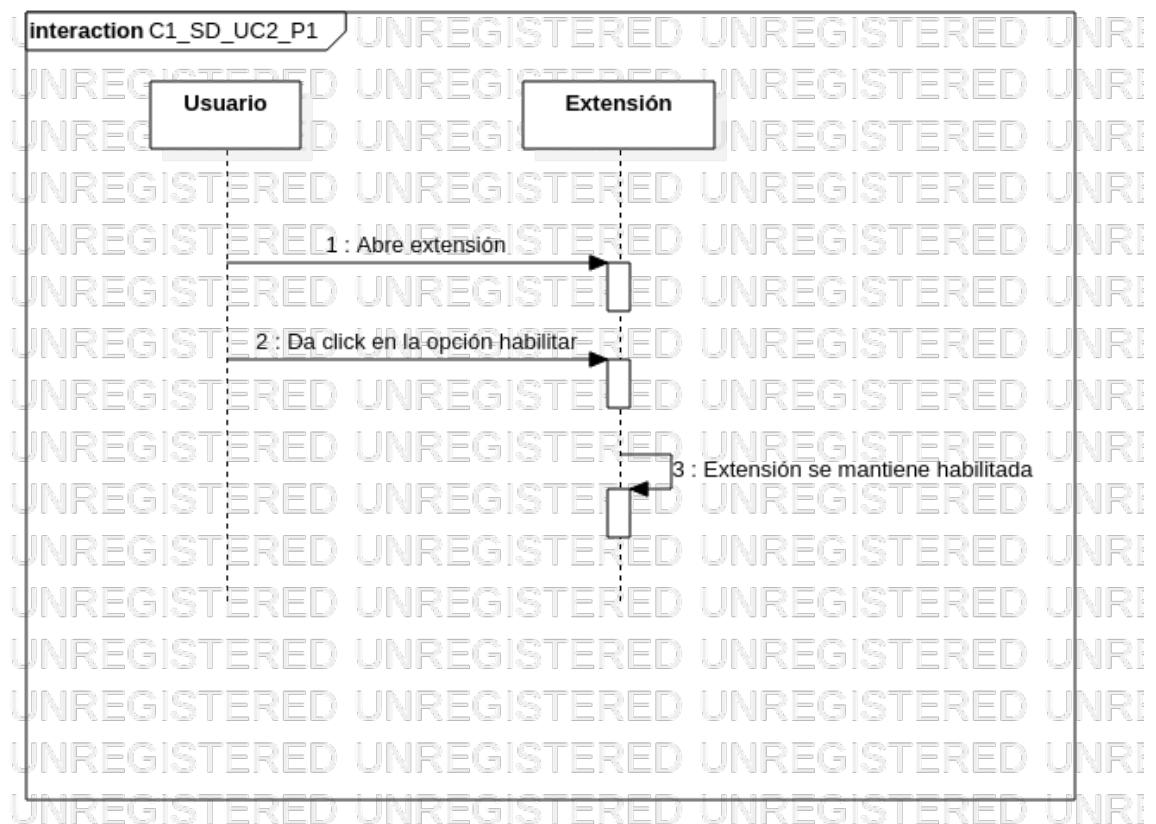


Figura 4.6: Diagrama de secuencia del CI_CU2. Habilitar extensión.

Descripción: Para habilitar la extensión, el usuario necesita primero abrir la extensión. Una vez abierta la extensión, debe de dar click en el botón 'habilitar', para que la extensión ejecute la orden y se mantenga habilitada.

4.1.6.3. Diagrama de secuencia 3

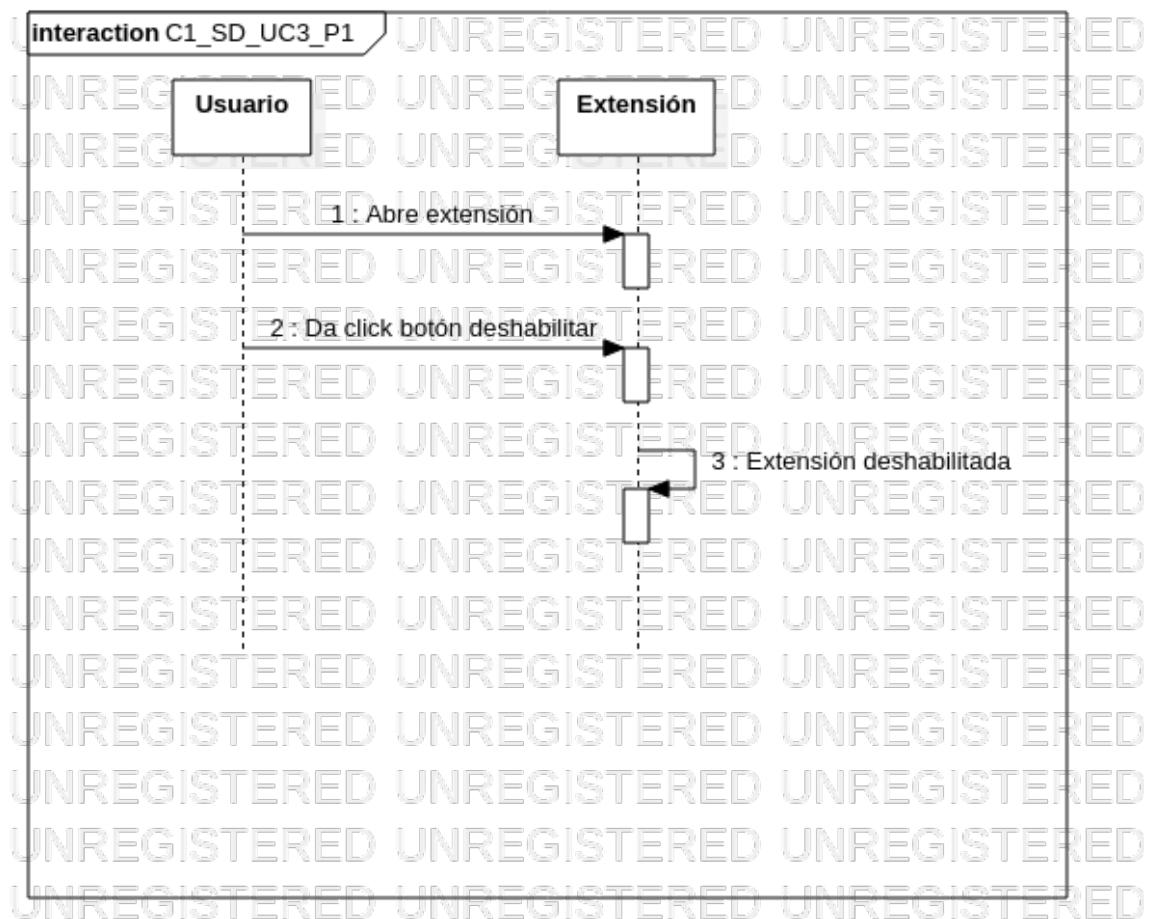


Figura 4.7: Diagrama de secuencia del CI_CU3. Deshabilitar extensión.

Descripción: Para deshabilitar la extensión, el usuario necesita primero abrir la extensión. Una vez abierta la extensión, debe de dar click en el botón "deshabilitar", para que la extensión ejecute la orden y se mantenga deshabilitada.

4.1.6.4. Diagrama de secuencia 4

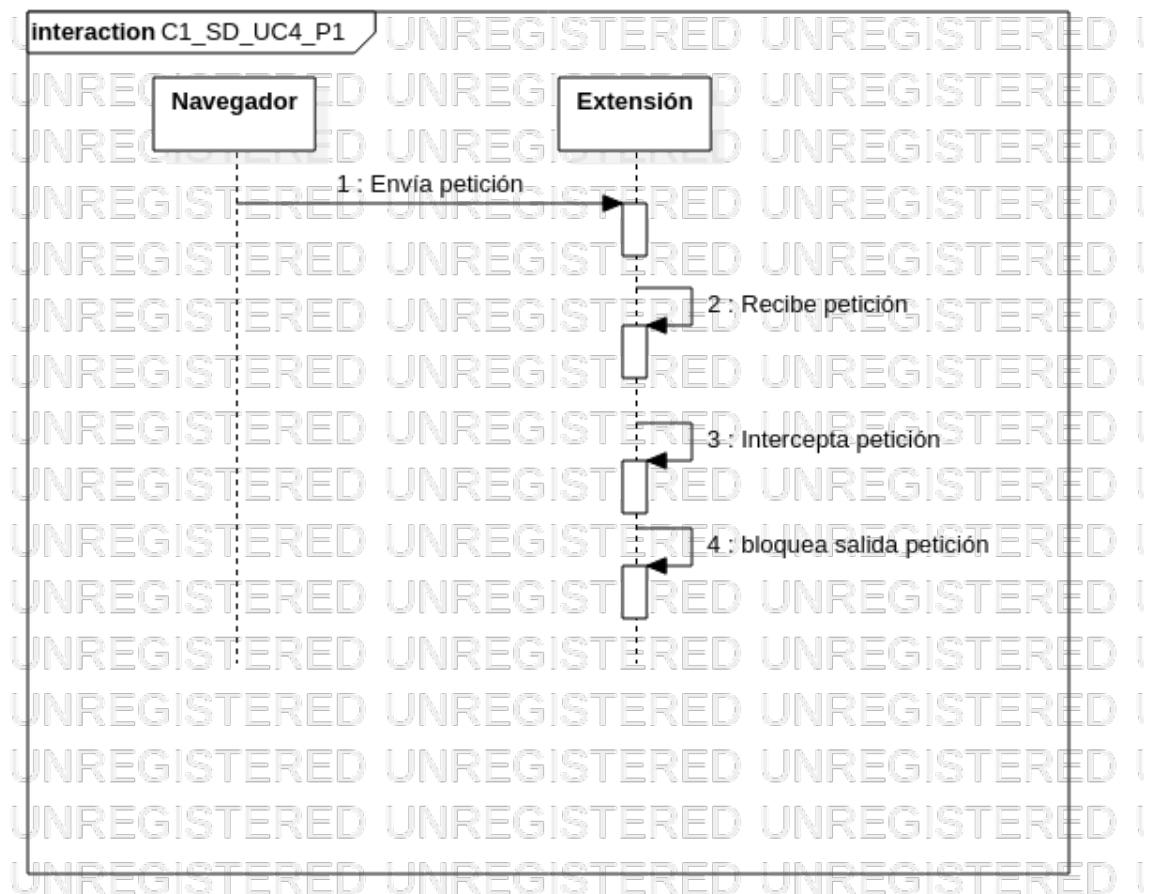


Figura 4.8: Diagrama de secuencia del CI_CU4. Interceptar petición.

Descripción: Una vez que el navegador ha enviado la petición, la extensión la interceptará. Lo primero que hace la extensión para conseguirlo es recibir la petición y bloquear su salida. Con ello la petición jamás saldrá a red y por ende no llegará al servidor.

4.1.6.5. Diagrama de secuencia 5.

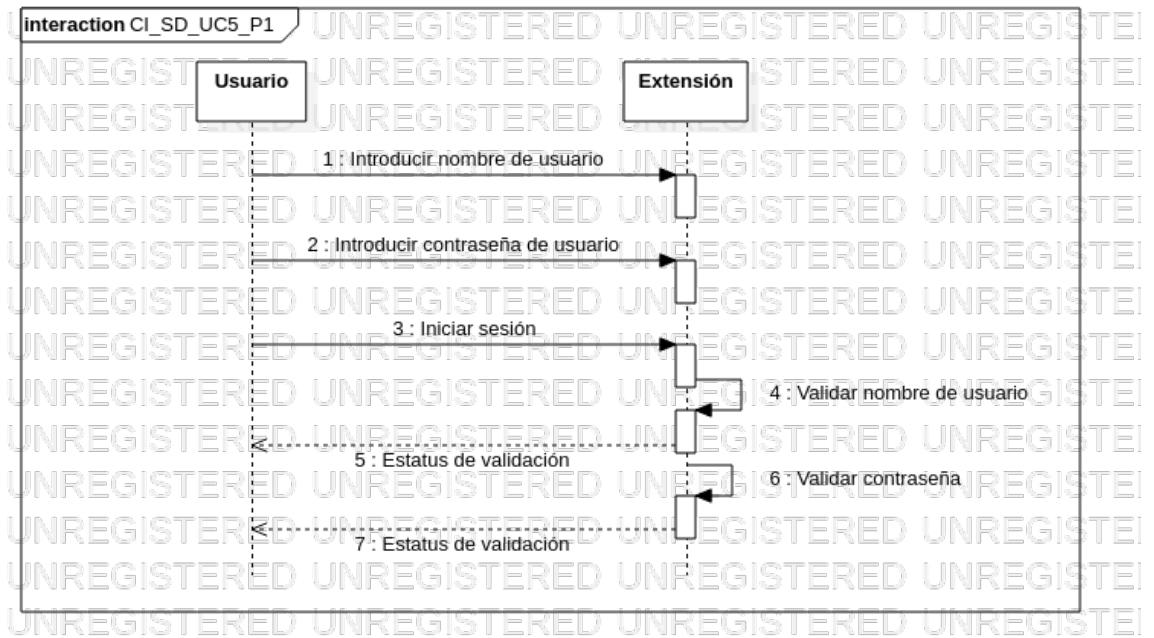


Figura 4.9: Diagrama de secuencia del CI_CU5. Inicio de sesión en la extensión.

Descripción: como primeros dos pasos de la secuencia para iniciar sesión en la extensión, el usuario ingresa su nombre de usuario y su contraseña, para después iniciar sesión en la extensión. Una vez que el usuario ha dado la orden de iniciar sesión, la extensión valida el nombre de usuario y la contraseña, retornando un mensaje en caso de que alguno de estos dos valores esté mal.

4.1.6.6. Diagrama de secuencia 6.

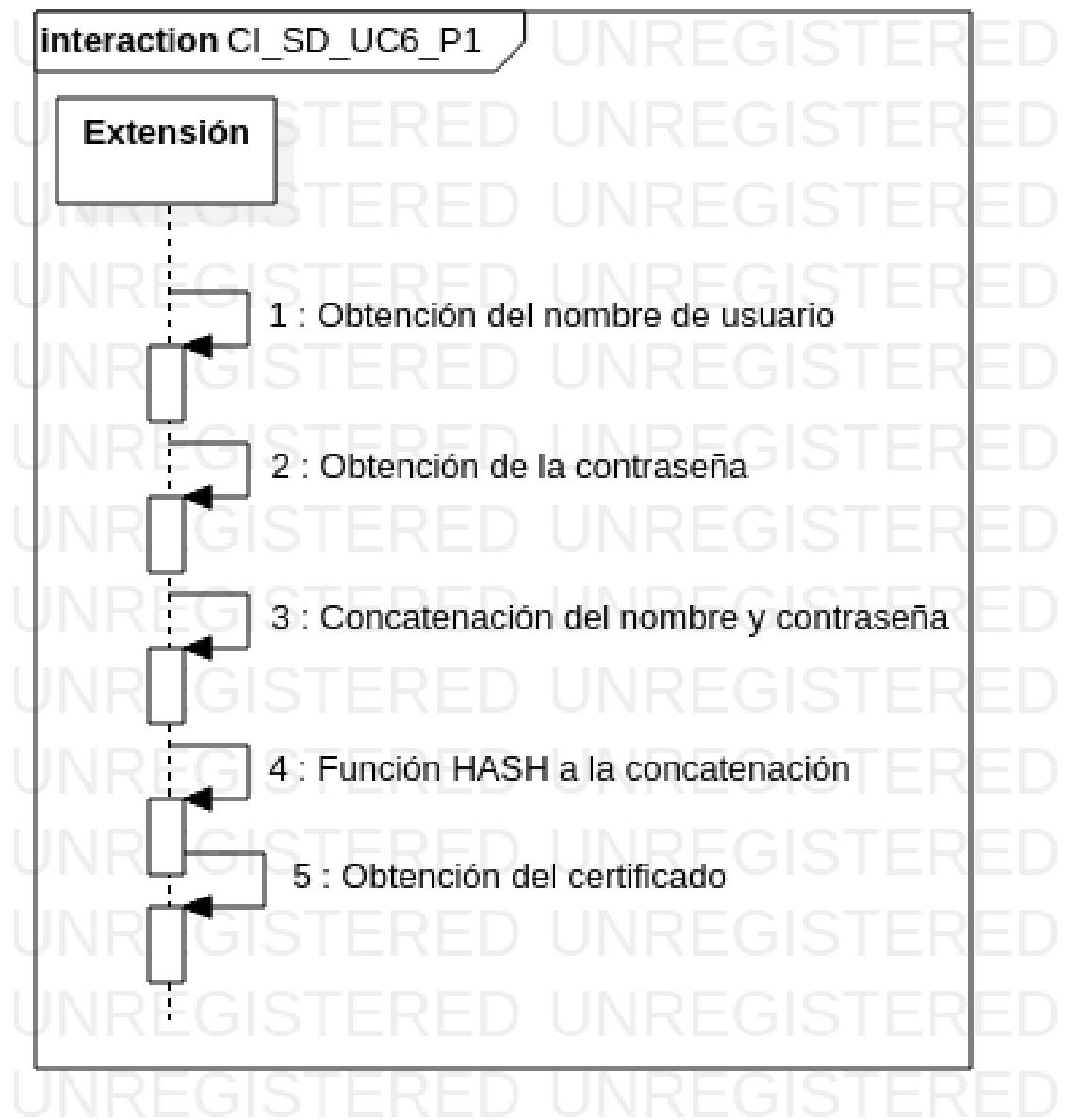


Figura 4.10: Diagrama de secuencia del CI_CU6. Generación del certificado autentificador.

Descripción: Una vez que el usuario ha iniciado sesión, la extensión procede a generar el certificado autentificador. Para ello se obtienen el nombre y la contraseña de usuario para concatenarlos en una única cadena y mandarlos a una función que genere un código HASH (sólo en este prototipo), para después obtener el certificado autentificador.

4.1.6.7. Diagrama de secuencia 7.

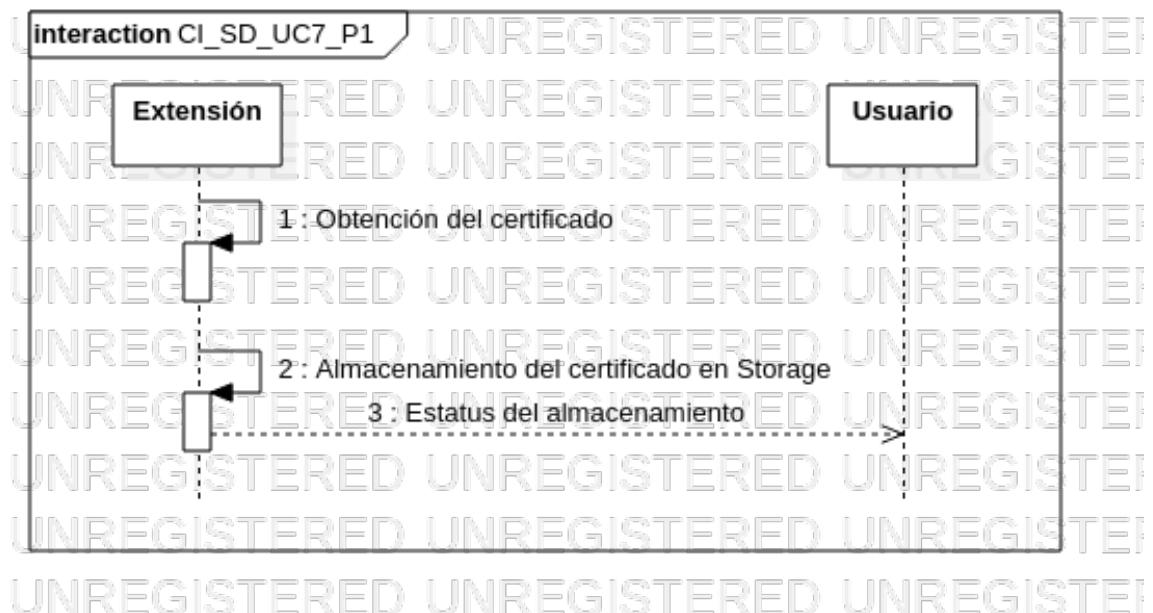


Figura 4.11: Diagrama de secuencia del CI_CU7. Almacenamiento del certificado autentificador.

Descripción: Una vez que se ha generado el código autentificador, es necesario almacenarlo en el Storage de la extensión, para ello la extensión abre una nueva entrada en el Storage y almacena el certificado en ella. Finalmente, la extensión retorna un mensaje del estatus del almacenamiento, para que el usuario se entere si fue exitoso o no.

4.1.6.8. Diagrama de secuencia 8.

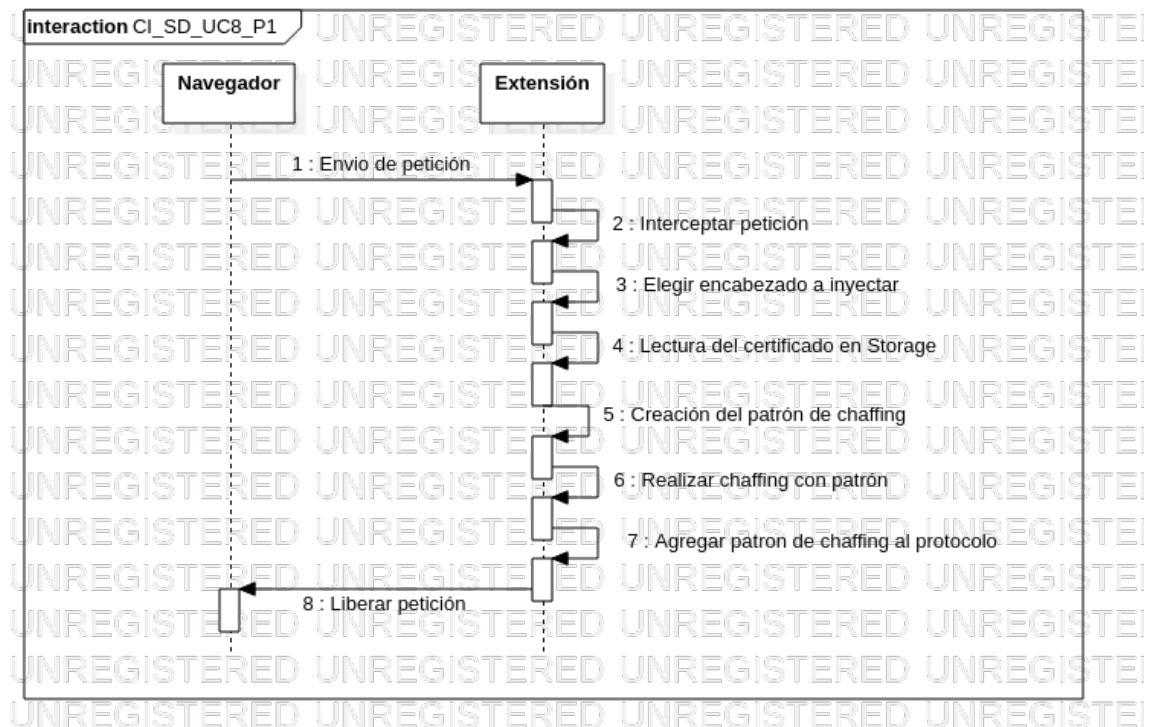


Figura 4.12: Diagrama de secuencia del CI_CU8. Generación del chaffing.

Descripción: Cuando un usuario haga una petición, el navegador enviará dicha petición al servidor correspondiente. Sin embargo, en este momento es cuando la extensión interviene para realizar los pasos necesarios para generar el chaffing. Primeramente, la extensión intercepta la petición para elegir el encabezado a injectar. Una vez que ha elegido el encabezado, busca obtener el certificado autentificador del Storage, para con base en él, crear el patrón de chaffing con el que se realizará la etapa de chaffing. Finalmente, la extensión agrega el patrón generado a una nueva entrada en el encabezado HTTP interceptado y le manda la señal al navegador para que éste la mande nuevamente.

4.1.6.9. Diagrama de secuencia 9.

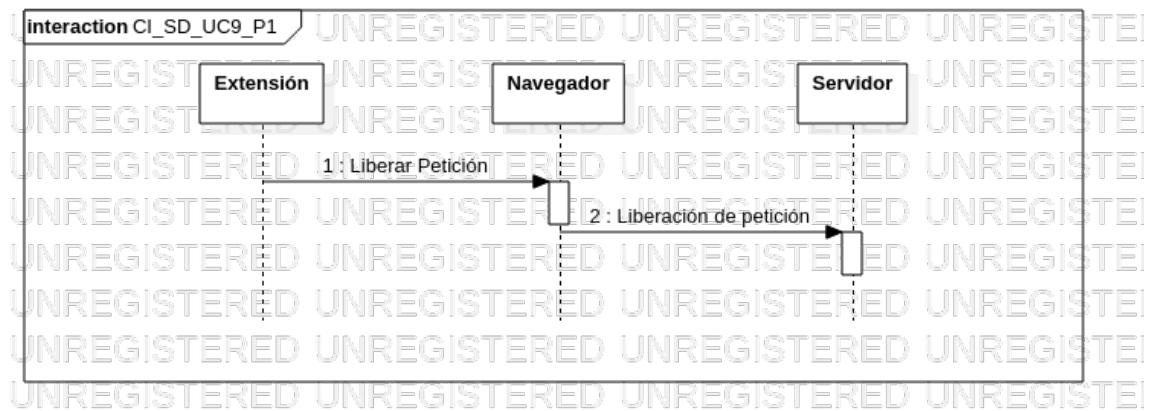


Figura 4.13: Diagrama de secuencia del CI_CU9. Liberación de la petición.

Descripción: El navegador una vez que recibe la señal de liberar petición, simplemente tiene que ejecutar su funcionamiento de 'realizar petición' para que ésta salga a red y busque llegar a su destino.

4.1.7. Diagrama de actividades

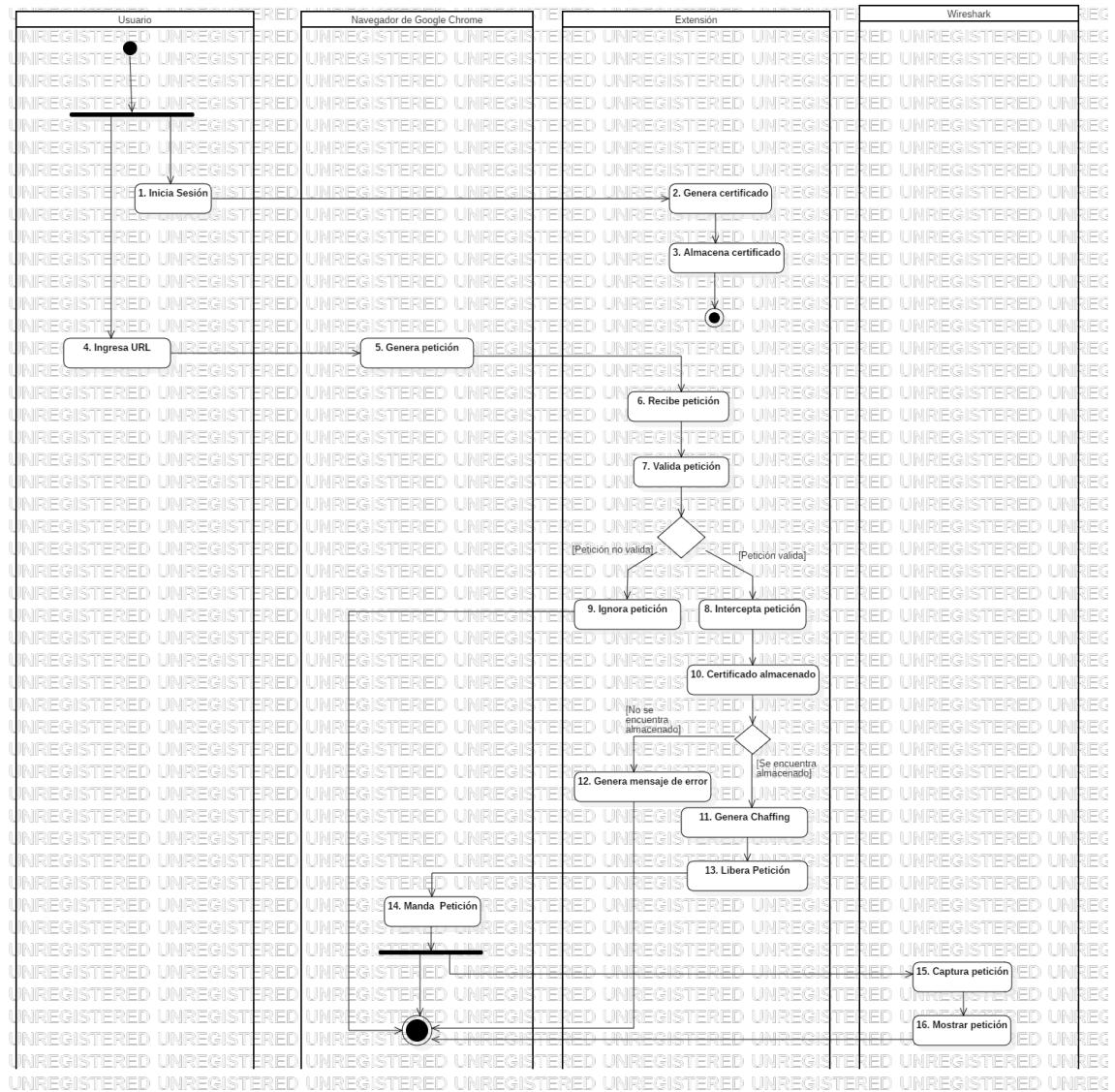


Figura 4.14: Diagrama de actividades del Prototipo 2.

4.1.7.1. Descripción del diagrama de actividades.

El componente cuenta con los siguientes pasos. Uno de los primeros pasos que debe hacer el usuario es iniciar sesión, esto con el fin de generar un certificado de acuerdo a los datos del usuario. Dicho certificado se almacena en el **Storage** de Google Chrome.

El otro camino a seguir por el usuario es realizar una búsqueda en el navegador, en la cual el navegador realiza la petición y la extensión recibe la misma. Modificándola siempre y cuando se encuentre un certificado guardado en el Storage. Si este proceso es válido, se genera el proceso de Chaffing y se libera la petición. El servidor se encarga de mandar dicha petición almacenada y en donde el analizador *Wireshark* se encarga de capturar la petición para mostrarla.

4.1.8. Interfaz de usuario.

4.1.8.1. Pantalla Inicial.

Esta pantalla es la primer vista que el usuario tiene el sistema. Aparece al darle click a la extensión en su ícono correspondiente. En ella, el usuario puede activar y desactivar la extensión para empezar a cachar peticiones, ademas cuenta con un botón de inicio de sesión (*Iniciar Sesión*), el cual al darle click abrirá la pantalla 'Tab de la extensión' (Figura 4.16). La Figura 4.15, muestra como se ve la pantalla inicial.



Figura 4.15: Pantalla inicial.

4.1.8.2. Tab de la extensión.

Esta pantalla es la interfaz que se le brinda al usuario para que inicie sesión y obtenga su certificado autenticador. La Figura 4.16 muestra la pantalla. En ella se aprecian únicamente dos campos para introducir texto ('Ingrese su Usuario' e 'Ingrese su contraseña'), y un botón 'Iniciar Sesión'.

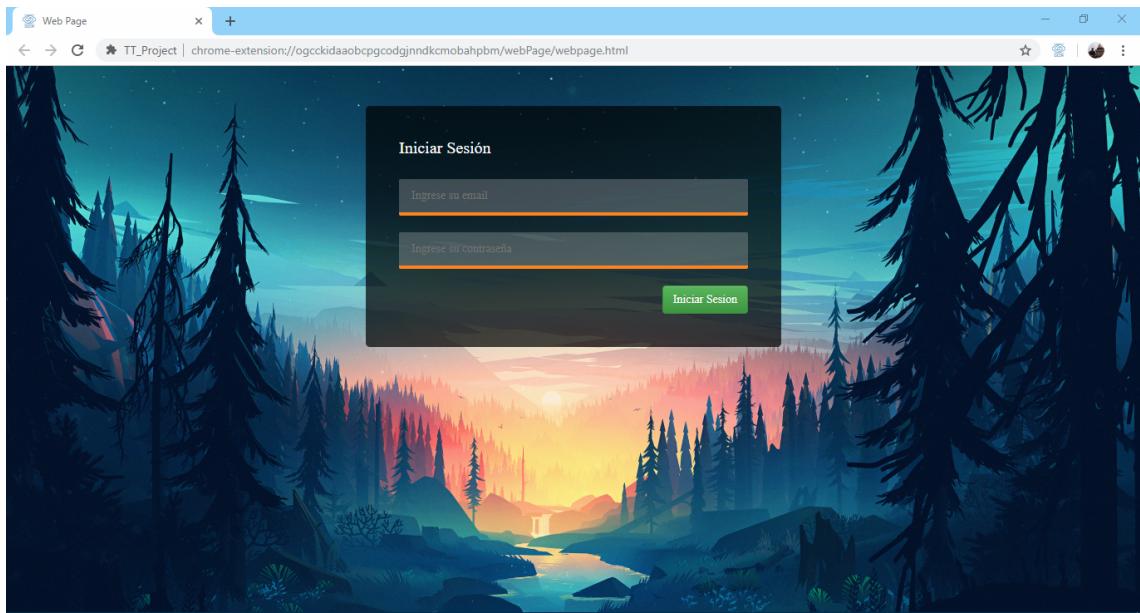


Figura 4.16: Tab de la extensión. Permite inicio de sesión

4.1.8.3. Mensajes de estado.

Los mensajes de estado, son mensajes que notifican al usuario errores, éxitos o problemas que se presentan al momento de realizar una acción en la extensión. La Figura 4.17 muestra el mensaje que se muestra el usuario tras haber guardado el certificado autentificador con éxito en el Storage de la extensión. La Figura 4.18 notifica al usuario que existió un error al querer guardar el certificado en el Storage de la extensión. Finalmente, la Figura 4.19, muestra que hubo un problema al querer obtener el certificado del Storage de la extensión.



Figura 4.17: Mensaje de éxito al guardar el certificado en storage de la extensión.

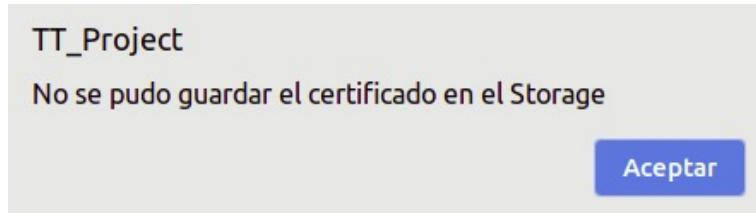


Figura 4.18: Mensaje de error al guardar el certificado en storage de la extensión.

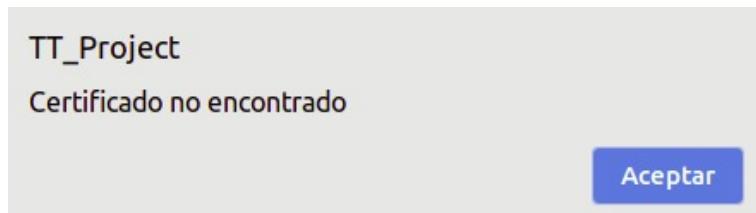


Figura 4.19: Mensaje de error al obtener certificado del storage de la extensión.

4.1.9. Requisitos de diseño.

En este apartado, se especificarán los requisitos de diseño para que el prototipo opere de forma correcta, de igualmanera se tiene por entendido que son necesarios los Requisitos del diseño del primer prototipo.

4.1.9.1. Requisitos de ejecución de la extensión

Para poder ejecutar el prototipo dos es necesario contar con todo lo requerido para el prototipo uno y agregarle la interacción con **jQuery 3.3.1** y **Bootstrap** que son dos poderosos frameworks que corren sobre JavaScript y que nos permiten interactuar un poco mejor con el usuario haciendo la interfaz de la extensión más amigable y entendible, estos ya se encuentran insertados en la extensión por lo que no es necesario que el usuario realice acción alguna. Otros de los requisitos para su ejecución es contar con un **usuario y contraseña** válidos ya que serán de suma Para deshabilitar la extensión, el usuario necesita primero abrir la extensión. Una vez abierta la extensión, debe de dar click en el botón "deshabilitar", para que la extensión ejecute la orden y se mantenga deshabilitada.

importancia para el correcto funcionamiento del prototipo dos.

4.1.9.2. Requisitos para el envío del código autentificador

Para este prototipo se considera necesaria los siguientes requisitos de diseño:

- **Código Autentificador** Archivo indispensable en este prototipo debido a que sin este es imposible acompletar el proceso.
- **Iniciar Sesión** Este botón generará un certificado de prueba y se almacenará en el Storage del navegador Google Chrome. Esto con el fin, que al momento de cachar la petición, la extensión de encargará de inyectar el certificado almacenado modificado con el método *Chaffing* en el encabezado de protocolo HTTP.

4.1.10. Algoritmos.

Los algoritmos necesarios para hacer el *chaffing* son expuestos a continuación:

```
Data: requestHTTP, cert
Result: patternChaffing
1 lenHTTP  $\leftarrow$  lenght(requestHTTP);
2 lenCert  $\leftarrow$  lenght(cert);
3 lenPattern  $\leftarrow$  lenHTTP + lenCert;
4 patternChaffing[lenPattern];
5 count  $\leftarrow$  0;
6 y  $\leftarrow$  lenHTTP % 8;
7 while count < lenCert do
8   x  $\leftarrow$  random % lenPattern;
9   if x  $\leq$  0  $\&\&$  x  $<$  8 - y  $\&\&$  y not 0 then
10    | continue;
11   end
12   if patternChaffing[x] == 0 then
13    | patternChaffing[x]  $\leftarrow$  1;
14    | count  $\leftarrow$  count + 1;
15   end
16 end
17 byteControl  $\leftarrow$  8 - y;
18 putFirst(patternChaffing, byteControl);
```

Algoritmo 1: Generación de patrón de chaffing

```

Data: requestHTTP, cert, patternChaffing
Result: protocolChaffed

1 lenPattern  $\leftarrow$  lenght(PatternChaffing);
2 protocolChaffed[lenPattern] countHTTP  $\leftarrow$  0;
3 countCert  $\leftarrow$  0;
4 controlByte  $\leftarrow$  getFirstByte(patternChaffing);
5 entero  $\leftarrow$  byteToInt(controlByte);
6 countProtocolChaffed  $\leftarrow$  entero;
7 while countProtocolChaffed  $<$  lenPattern do
8   if protocolChaffed[countProtocolChaffed] == 0 then
9     protocolChaffed[countProtocolChaffed] = cert[countCert];
10    countCert  $\leftarrow$  countCert + 1;
11  else
12    protocolChaffed[countProtocolChaffed] =
13      requestHTTP[countHTTP];
14    countHTTP  $\leftarrow$  countHTTP + 1;
15  end
16  countProtocolChaffed  $\leftarrow$  countProtocolChaffed + 1;
17 end

```

Algoritmo 2: Generación de chaffing

Primero vamos a analizar el algoritmo del *patrón de chaffing* con un pequeño ejemplo (utilizaremos datos de variables más cortos); supongamos que nuestro certificado es el siguiente:

$$C_k = MITZ057abZ251$$

y utilizaremos el campo *agent user* del header de la petición, lo cual tendrá lo siguiente:

$$P_{HTTP} = Mozilla5,5/Chrome8,1/Safari$$

Entonces, nuestro patrón de chaffing terminará teniendo un tamaño de la longitud de los caracteres de nuestro certificado + la longitud de los datos de la petición HTTP, que es nuestra variable *lenPattern*, y en este caso será de una longitud de 41. A continuación vamos a utilizar un arreglo de banderas de ese tamaño que inicia con 0 todos sus valores, y que al final será nuestro patrón, (variable *patternChaffing*).

La idea es generar posiciones aleatorias dentro del rango del tamaño de *lenPattern*, y poner un 1 en dicha posición si es que hay un 0, en caso de que

no se encuentre un 0 se repetirá el procedimiento obteniendo una posición aleatoria diferente, y esto se realizará el mismo número de veces del tamaño de nuestro certificado, para obtener un patrón de combinaciones entre los caracteres. Utilizaremos un contador para conseguir esto, aumentándolo cada vez que se obtenga un número aleatorio válido. En nuestro algoritmo, nuestra variable x contiene la posición aleatoria donde se validará si en esa posición se puede poner un 1 o no.



Figura 4.20: Arreglo del patrón de chaffing

Supongamos, por ejemplo, que el primer número aleatorio que se obtiene es 4, entonces en la posición 4 colocaremos un 1:



Figura 4.21: Arreglo del patrón de chaffing después de una iteración

Este algoritmo nos permite llenar de unos el número de veces del tamaño de nuestro certificado, lo que nos asegura que cada posición le corresponde a un carácter ya sea del certificado o de la petición a enviar. Supongamos que al terminar este algoritmo, nuestro arreglo queda algo parecido a lo siguiente:



Figura 4.22: Arreglo del patrón de chaffing final

El segundo algoritmo realizará el chaff utilizando el patrón generado en el algoritmo anterior, obtendrá el byte de control y a partir de este, comenzará un contador para recorrer todos los bytes del patrón de chaffing, ademas contaremos con otros 2 contadores más: *contCert* que irá recorriendo cada carácter de nuestro certificado, y *countHTTP* que recorrerá los de la petición HTTP. Si en la posición de éste contador se encuentra un 0, entonces quiere decir que debemos de agarrar el siguiente carácter de nuestro certificado, basándonos en el contador del certificado, de la misma manera si se encuentra un 1, se agarrará el siguiente carácter de la petición, y estos se irán concatenando en una nueva cadena (*protocolChuffed*).

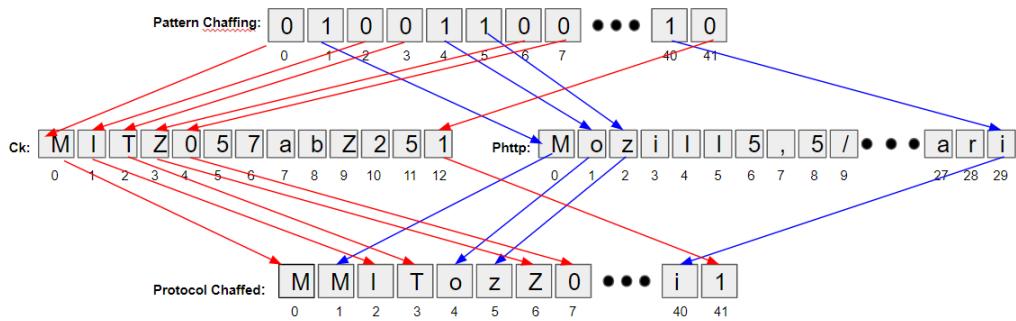


Figura 4.23: Arreglo chaff final.

Al final necesitaremos un byte de control que le servirá al servidor saber a partir de donde empezará a realizar el *winnowing*, esto se debe a que dependiendo del tamaño de la petición HTTP y su módulo 8 es donde empezará a checar los 0's y 1's; mandaremos este byte de control al principio de la petición con chaff.

Por último se enviará al servidor el patrón de chaffing junto con el mismo chaff, así podrá saber como realizar el *winnowing* para obtener los datos correspondientes del certificado.

Capítulo 5

Desarrollo

5.1. Componente I.

Para verificar que nuestro componente funciona correctamente procedemos a mostrar una prueba del funcionamiento del mismo.

Primeramente se necesita iniciar sesión en la extensión, esto con el fin de obtener un certificado y que el mismo se guarde en el storage de Google Chrome. En la prueba iniciamos sesión con los siguientes datos (Figura 5.1):

- **usuario:** usuarioPrueba
- **contraseña:** usuarioP1234@

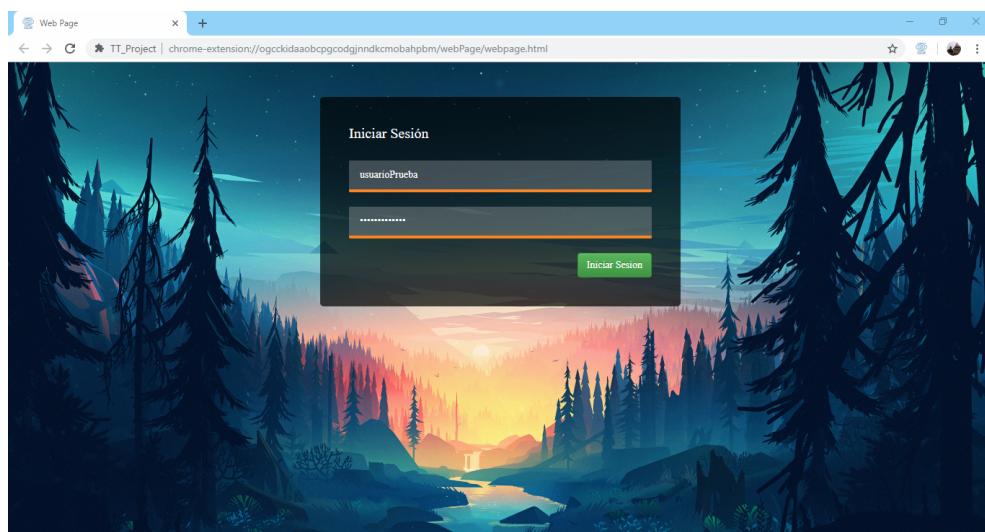


Figura 5.1: Inicio de sesión para la obtención del certificado.

Generando así el siguiente código hash:

1408810b7d854a723873e76dbfd989ade608daae

Como siguiente paso, este código hash se guarda en el *Storage* de Google Chrome y se da aviso del estado de este procedimiento (Figura 5.2).

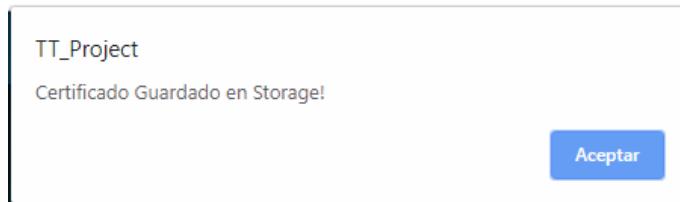


Figura 5.2: Aviso de guardado del certificado en Storage.

Una vez que el certificado se haya guardado con éxito en el *Storage* de Google Chrome, realizamos una búsqueda en Google Chrome, para esta prueba se hizo una petición a un servidor local, montado en *Apache Tomcat* previamente instalado en otra maquina dentro de una red LAN¹. Esta petición será bloqueada por la extensión, como en la Figura 5.3, para inyectar el código con *Chaffing* en el protocolo HTTP en el apartado de *headers*.

¹Una red de área local o LAN (Local Area Network) es una red de computadoras que abarca un área reducida a una casa, un departamento o un edificio.



La página 10.0.0.8 está bloqueada

Una extensión ha bloqueado el envío de solicitudes al servidor.

Inhabilita las extensiones.

ERR_BLOCKED_BY_CLIENT

[Volver a cargar](#)

Figura 5.3: Pagina bloqueada del lado del cliente.

Una vez injectado el certificado autenticador, se envía la petición con el protocolo modificado al servidor destino. Para verificar que a través de la red se envía la petición modificada se hace uso del analizador de paquetes Wireshark.

La Figura 5.4, muestra la petición enviada al servidor, donde en el apartado de *Hypertext Transfer Protocol* se observa que en **Accept** está injectado el certificado con *Chaffing* y en **Pattern** está injectado el patrón realizar el *winnowing* en el servidor (en el siguiente prototipo).

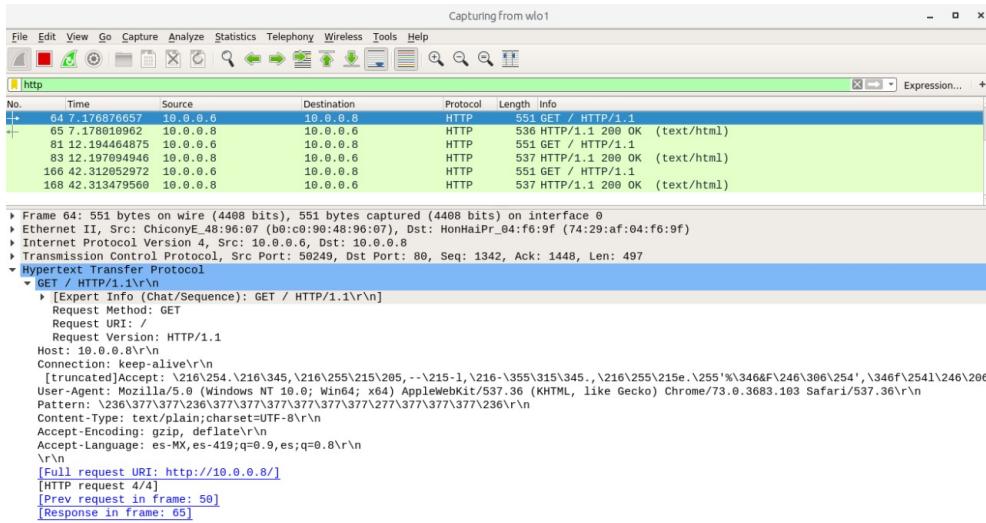


Figura 5.4: Wireshark analizando en red WI-FI filtrando análisis por *http*.

Para un análisis más específico, se muestra la petición en una herramienta que proporciona wireshark, *Show Packet Bytes...*, la cual muestra el encabezado completo, teniendo una herramienta para seleccionar la codificación del texto (Figura 5.5). Nosotros elegimos la codificación ISO8859-1, ya que en ésta nos permite ver de manera legible el encabezado.

Wireshark - Hypertext Transfer Protocol (http) · wlo1

```
GET / HTTP/1.1
Host: 10.0.0.8
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36
Pattern: \ÿÿÿÿÿÿÿÿ
Content-Type: text/plain;charset=UTF-8
Accept-Encoding: gzip, deflate
Accept-Language: es-MX,es-419;q=0.9,es;q=0.8
```

Frame 64, Hypertext Transfer Protocol (http), 497 byte(s).

Decode as: None Show as: ISO 8859-1 Start: 0 End: 497 Find Next
Find: Print Copy Save as... Cerrar Ayuda

Figura 5.5: Análisis de petición en *Show Packet Bytes...*

Capítulo 6

Avances y trabajo por hacer.

Actualmente hemos desarrollado dos prototipos que son necesarios para conocer el verdadero funcionamiento del sistema, por un lado el prototipo uno nos permite interceptar una petición HTTP con el objetivo de mostrarla para identificar en qué parte de la cabecera agregaremos la parte del código autenticador y cómo lo vamos a estructurar y por otro lado el prototipo dos en el cual realizamos el proceso de chaffing del código y su respectivo patrón y lo enviaremos por la red a un servicio web, logrando que estos datos lleguen de manera exitosa al otro servidor. Como segunda parte de este trabajo terminal se realizará el análisis y desarrollo de los prototipos 3 y 4 que representan dos de los bloques más importantes de este trabajo terminal, por el lado del prototipo 3 se implementará un servicio web que implementará una API con el propósito de realizar el Winnowing de la petición HTTP modificada por lo que implica una modificación al servidor Apache para que reconozca este tipo de peticiones, por otro lado se implementará un método de cifrado asimétrico mediante RSA para comunicar el patrón resultante de Chaffing de manera segura entre la extensión y el servicio web, de esta manera buscamos autenticar al usuario de manera rápida, eficiente y sencilla para los usuarios. Por otro lado el prototipo 4 consiste en la implementación de un servidor autenticador que será el encargado de crear y almacenar cada uno de los certificados correspondientes para cada usuario con el fin de que éstos los puedan obtener fácilmente en su extensión logrando que se puedan iniciar múltiples sesiones en diferentes extensiones, siempre cuidando que este certificado se encuentre lo más seguro posible. Como podemos analizar aún nos falta una gran parte de este extenso trabajo pero confiamos en nuestro equipo y en nuestra habilidad para poder resolver todas las problemáticas que se nos presenten en el camino.

Bibliografía

- [1] A. Aguilera Hernández (2014, abril 25), Sugerencias de Seguridad para Sitios Web, [En línea]. Disponible: <https://www.seguridad.unam.mx/historico/documento/index.html-id=1143>. [Último acceso: 15 de febrero del 2019].
- [2] J. R. Aguirre, *Seguridad Informática y Criptografía*, 2da edición, Madrid, España: Universidad Politécnica de Madrid, 2006.
- [3] M. Bellare y A. Boldyreva, "The Security of Chaffing and Winnowing", California, San Diego, 2015. Disponible: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.160.4853&rep=rep1&ttype=pdf>. [Último acceso: 5 de mayo del 2019].
- [4] A. Beutelspacher, *Cryptology*, edición 1994, Washington, Estados Unidos de América: Mathematical Association of America, 1994.
- [5] CCM (2017), El protocolo HTTP, [En línea]. Disponible: <https://es.ccm.net/contents/264-el-protocolo-http>. [Último acceso: 6 Mayo 2019].
- [6] S. Díaz Santiago, "Generacion De Sucesiones Criptográficamente Fuer tes", tesis de Maestría, División de ciencias básicas e ingeniería, UAM, D.F., México, 2005.
- [7] C. C. Espinosa Madrigal (2011, junio 16), Robo de Identidad y Consecuencias Sociales, [En línea]. Disponible: <https://www.seguridad.unam.mx/historico/documento/index.html-id=16?fbclid=IwAR0u8WAXORvBxZ3H-aMzlBhd-6o7g8ycS88eRu7nY1t1XVtCufhEcQ7hWDs>. [Último acceso: 15 de febrero del 2019].
- [8] T. Fisher (2019), What Is SHA-1 and How Is It Used for Data Verification?, [En línea]. Disponible: <https://www.lifewire.com/what-is-sha-1-2626011>. [Último acceso: 5 mayo 2019].

- [9] J. D. Gauchat, *El gran libro de HTML5, CSS3 y Javascript*, 1ra edición, Barcelona, España: MARCOMBO S.A., 2012.
- [10] S. Goldwasser y S. Micali, "Probabilistic encryption", *Journal of Computer and System Science*, vol. 28, no. 4, pp. 270–299, 1984.
- [11] Google code (2019), crypto-js, [En línea]. Disponible: <https://code.google.com/archive/p/crypto-js/>. [Último acceso: 5 de mayo del 2019].
- [12] IBM Community (2019), TRIRIGA Wiki Home, [En línea]. Disponible: <https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/IBM%20TRIRIGA1>. [Último acceso: 5 mayo 2019].
- [13] IBM (2019), IBM TRIRIGA Application Platform, [En línea]. Disponible: https://www.ibm.com/support/knowledgecenter/es/SSHEB3_3.6.0/com.ibm.tap.doc/sso_topics/t_ctr_authenticate.html. [Último acceso: 5 mayo 2019].
- [14] J. Pacheco (2018, julio 18), Entre cookies y privacidad, Oficina de Seguridad del Internauta, [En línea]. Disponible: <https://www.osi.es/es/actualidad/blog/2018/07/18/entre-cookies-y-privacidad>. [Último acceso: 5 de mayo del 2019].
- [15] A. Komarova y A. Menshchikov, "Comparison of Authentication Methods on Web Resources" en Proceedings of the Second International Scientific Conference "Intelligent Information Technologies for Industry", Varna, Bulgaria, 14–16 Septiembre, 2017, pp 106-120.
- [16] J. Larkin, "Implementation of Chaffing and Winnowing: providing confidentiality without encryption", tesis de Licenciatura en Ciencias de la Computación, University of Bath Bath, Inglaterra, 2006. [En línea]. Disponible: <https://pdfs.semanticscholar.org/5520/1a43a747f4a3fb554f241c7b7bc7636b4a07.pdf>. [Último acceso: 5 de mayo del 2019].
- [17] A. Maiorano, *Criptografia: Tecnicas De Desarrollo Para Profesionales*, 1ra edición, D.F., México: Alfaomega, 2009.
- [18] A. Maurya1, P. Kumar Saini y N. Goel, "Chaffing and Winnowing without using steganography and encryption technique", *International*

Journal of Information Technology and Knowledge Management, vol. 4, no. 4, pp 515-517, Diciembre, 2011

- [19] A. J. Menezes, P. v. Oorschot y S. Vanstone, *Handbook of Applied Cryptography*, 1ra edición, Florida, Estados Unidos de América: CRC Press, 1996.
- [20] Mozilla (2019, mayo 2), JavaScript. [En línea]. Disponible: <https://developer.mozilla.org/en-US/docs/Web/JavaScript> [Último acceso: 5 de mayo del 2019].
- [21] Mozilla, (2019, 19 marzo), FileSystem, [En línea]. Disponible: <https://developer.mozilla.org/es/docs/Web/API/FileSystem>. [Último acceso: 5 de mayo del 2019].
- [22] R. S. Pressman, *Ingeniería del Software. Un enfoque práctico*, 7ma edición, D.F, México: McGraw-Hill, 2010.
- [23] R. L. Rivest, "Chaffing and Winnowing: Confidentiality without Encryption", Laboratorio de ciencias de la computación del MIT, Massachusetts, Estados Unidos de América, 1998.
- [24] A. Romero Mier y Terán y M. A. Vasquéz Martínez (2016, abril 19), Aspectos Básicos de la Seguridad en Aplicaciones Web. [En línea]. Disponble: <https://www.seguridad.unam.mx/historico/documento/index.html-id=17>. [Último acceso: 5 de mayo del 2019].
- [25] Universidad Politécnica de Madrid (2004), Criptografía, [En línea]. Disponible: http://www.dma.fi.upm.es/recursos/aplicaciones/mathematica_discreta/web/aritmetica_modular/criptografia.html. [Último acceso: 5 de mayo del 2019].
- [26] VeriSign Inc. (2019), Todo lo que debe saber sobre certificados SSL, [En línea]. Disponible: https://www.verisign.com/es_LA/website-presence/online/ssl-certificates/index.xhtml. [Último acceso: 5 de mayo del 2019].
- [27] Wireshark (2019), What is Wireshark?, [En línea]. Disponible: https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html#ChIntroWhatIs. [Último acceso: 20 abril 2019].
- [28] Kerberos (2019), Descripción del Kerberos un servicio de autenticación para los sistemas de red abierta, [En línea]. Disponible: https://www.cisco.com/c/es_mx/support/docs/security-vpn/kerberos/16087-1.html#whatisit

- [29] Van Tilborg, Henk C.A, "Encyclopedia of Cryptography and Security". *Eindhoven University of Technology The Netherlands*, United States of America, Editorial Springer, 2005, 671 pag.
- [30] <http://www.itefi.csic.es/sites/default/files/hernandez-encinas/firma-y-certificado-electronico.pdf>
- [31] <https://www.uv.es/uvweb/universidad/es/politica-privacidad/politica-cookies/son-cookies-1285919089226.html>