INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE CÓMPUTO

Trabajo Terminal I.

# Autentificación Mediante Chaffing And Winnowing En El Protocolo HTTP

2018-B003.

---


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

Directores:
Moreno Cervantes Axel Ernesto
Díaz Santiago Sandra

# Índice

# Índice de figuras.

# Índice de cuadros.

# Capítulo 1.

## 1. Introducción.

«“‘¡HEAD En la actualidad los usuarios de internet necesitan guardar contraseñas para sus distintas cuentas en las diferentes páginas web en las que ingresa ya que recordarlas es un problema que avanza constantemente. El uso constante de contraseñas incita a los usuarios a guardar sus contraseñas en medios fisicos o digitales y perderlos presenta un grave problema de seguridad. La gran mayoria de servicios web han implementado una solución la cual es recordar tu usuario y contraseña para qué el usuario pueda acceder automaticamente al servicio. Dicha solucion presenta cierta vulnerabilidad ya que los archivos donde se guarda la información se pueden copiar y con ello replicarlo a otro ordenador.

»”’Las contraseñas son usadas principalemente en correos electrónicos, redes sociales, bancos en linea, entre otros importantes sitios web. Por lo que el robo de las mismas puede poner en riesgo la seguridad del usuario e ingresar sus datos de usuario y contraseña en cada sesion pueden ser faciles de robar dado qué, quedan a la vista de las personas de su alrededor. Cómo se menciono anteriormente las contraseñas son comúnmente utilizadas para el inicio de sesión y éstas deben contener multiples caractéres para así ser más seguras pero al mismo tiempo se vuelven más complicadas al momento de recordarlas.

»”’Es por ello, que en este trabajo terminal, propone una forma de autentificación por medio de Chaffing and Winnowing y con la ayuda de una extensión de Google Chrome, el cual servirá para la inyección de las credenciales de Login del usuario en el protocolo HTTP, y así, si un servicio web tiene éste tipo de seguridad disponible lo pueda validar.

»”’Este trabajo, tiene como objetivo, mejorar los aspectos antes mencionados como lo son la comodidad de recordar contraseñas y la seguridad. Gracias a éste proyecto el usuario podrá ingresar a sus páginas favoritas sin la necesidad de ingresar su usuario y contraseña constantemente, y con la seguridad de que sus contraseñas no seran robadas ya que no se almacenarán en ningún sitio o documento dentro del ordenador del usuario.

»”’=======

## »”’1.1. Planteamiento del problema.

»”’En la actualidad todos los usuarios de internet necesitan guardar contraseñas para sus distintas cuentas en las diferentes páginas web en las que ingresa ya que recordarlas es un problema que avanza constantemente. El uso de estas contraseñas son utilizadas principalmente en correos electrónicos y redes sociales por lo que el robo de las mismas puede poner en riesgo la seguridad del usuario, así como también, existe la tediosa tarea de ingresar usuario y contraseña en cada sesion. Las contraseñas son comúnmente utilizadas para el inicio de sesion y existen diferentes métodos de autentificación para dicho inicio como lo son biométricos. En nuestro proyecto nos enfocaremos más en el uso de text password en donde se autentificará el usuario por medio de una extensión de Google Chrome. Con ayuda de esta extensión resolveremos los problemas comentados anteriormente, dando así comodidad y seguridad al usuario que habilite la extensión.

## »”’1.2. Justificación.

»”’Los usuarios deben de guardar las contraseñas en medios fisicos o digitales y perderlos presenta un grave problema de seguridad. La gran mayoria de servicios web han implementado una solución la cual es recordar tu usuario y contraseña para que se pueda automaticamente acceder al servicio. Dicha solucion presenta cierta vulnerabilidad ya que los archivos donde se guarda la información se puede copiar y con ello replicarlo a otra computadora. En el cuadro No.1, se muestra una tabla donde se comparan los diferentes métodos de autentificación basándose en la simplicidad de su aplicación para el usuario (extraída del artículo Comparison of Authentication Methods on Web Resources). Donde: 1 – Bajo desempeño, 2 - Medio desempeño y 3 – Alto desempeño.

»”’La tabla anterior concentra las siguientes caracteristicas:

- ’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.

| | 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 dinamicas | 1 | 3 | 2 | 2 | 3 | 2 | 2 |
| Tokens | 3 | 1 | 1 | 2 | 2 | 3 | 1 |
| Multivariación | 1 | 1 | 1 | 3 | 2 | 2 | 1 |
| Cryptografía | 3 | 1 | 1 | 1 | 1 | 2 | 1 |
| Biométricos | 3 | 3 | 2 | 3 | 2 | 2 | 1 |

»”’Cuadro 1: Comparación de la aplicación en los distintos métodos de autentificación

- ’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 No.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 dinamicas | 2 | 3 | 2 | 2 |
| Tokens | 3 | 3 | 3 | 3 |
| Multivariación | 1 | 1 | 3 | 3 |
| Cryptografía | 3 | 3 | 3 | 3 |
| Biométricos | 3 | 3 | 1 | 1 |

»”’Cuadro 2: Comparación de la seguridad en los dstintos 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.

»"""»¿6101f1a0c0bd5ca44689803a36837e5988443337

## 1.3. Objetivos.

### 1.3.1. Objetivo general.

Realizar una extensión en Google Chrome que implemente un mecanismo de autentificación, implementando *Chaffing and Winnowing*.

### 1.3.2. 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 código (la autentificación) en el encabezado HTTP para enviar la petición al servidor.
- 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.

## 1.4. Metodología.

## 1.5. Estado del Arte.

# 2. Marco Teórico.

Como sabemos hasta ahora haremos uso de una extensión de Google Chrome, por lo que empecemos explicando que son estas extensiones. Una extensión de Google Chrome es una pequeña aplicación que se instala en el navegador que, en cierta medida, mejora la navegación del usuario. Estas extensiones tienen diferentes funcionalidades, que, como se dijo anteriormente, facilitan al usuario durante su navegacion por la internet. Existen una infinidad de extensiones hoy en día con funcionalidades inimaginables para distintas paginas, redes sociales, media, etc. La instalación de las extensiones es muy fácil gracias a Chrome Web Store. Como sabemos, Chrome Web Store es una tienda en línea de aplicaciones web para el navegador Google Chrome, y la cual es desarrollada y mantenida por Google (La tienda también cuenta temas visuales para el navegador). Esta tienda es mas intuitiva y amigable para cualquier usuario, facilitando la instalción de las extensiones con un simple click. «“‘¡HEAD

»”’En el cuadro No.1, se muestra una tabla donde se comparan los diferentes métodos de autentificación basándose en la simplicidad de su aplicación para el usuario (extraída del artículo Comparison of Authentication Methods on Web Resources). Donde: 1 – Bajo desempeño, 2 - Medio desempeño y 3 – Alto desempeño.

| | 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 dinamicas | 1 | 3 | 2 | 2 | 3 | 2 | 2 |
| Tokens | 3 | 1 | 1 | 2 | 2 | 3 | 1 |
| Multivariación | 1 | 1 | 1 | 3 | 2 | 2 | 1 |
| Cryptografía | 3 | 1 | 1 | 1 | 1 | 2 | 1 |
| Biométricos | 3 | 3 | 2 | 3 | 2 | 2 | 1 |

»”’Cuadro 3: Comparación de la aplicación en los distintos métodos de autentificación

»”’La tabla anterior concentra las siguientes caracteristicas:

’▪ 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 No.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 dinamicas | 2 | 3 | 2 | 2 |
| Tokens | 3 | 3 | 3 | 3 |
| Multivariación | 1 | 1 | 3 | 3 |
| Cryptografía | 3 | 3 | 3 | 3 |
| Biométricos | 3 | 3 | 1 | 1 |

»”’Cuadro 4: Comparación de la seguridad en los dstintos 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.

»”’=======
»”””»¿6101f1a0c0bd5ca44689803a36837e5988443337

# 3. Análisis.

## 3.1. Prototipo I.

### 3.1.1. Descripción.

En este prototipo se busca la creación de una extensión de Google Chrome, que sea capaz de interceptar una petición HTTP hecha por el navegador.

### 3.1.2. Herramientas a usar.

**Software.**
Para el desarrollo de software de este prototipo, ocuparemos las siguientes tecnologías debido a que nos facilitan el desarrollo y nos proporcionan lo necesario para lograr nuestro objetivo para este prototipo:

**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 hámbito 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 aproximacción a un uso real fué en mayor parte para ”dar vida a una página web”, como dar animaciones a un boton, interacciones en tiempo real, entre otras más. JavaScript fué desarrollado por NetScape, a partir del lenguaje Java, que en ese momento éste lenguaje tenía mucho auge y popularidad, y su principal diferencia es que JavaScript solo ”funciona”dentro de una página HTML.
JavaScript fué declarado como estándar del European Computer Manufacturers Association (ECMA) en 1997, y poco despúes también fué estandarizado por ISO.[3]

**Hardware.**
En el ambito del hardware utilizaremos los equipos de cómputo con los cuales contamos actualmente los integrantes, donde se especificaran a continuación:

| Equipo de hardware utilizado. | |
|---|---|
| Nombre | Morales González Diego Arturo |
| 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. | |
|---|---|
| Nombre | Carrillo Fernández Gerardo |
| Marca | HP |
| Modelo | Pavilion g4 |
| Procesador | Intel Core i3 |
| Tarjeta de video | Intel Sandybridge Mobile |
| Memoria RAM | 6 GB |
| Disco duro | 500GB |

### 3.1.3. Estudio de requerimientos.

**Requerimientos Funcionales.**

**PI_RF1. Interceptar petición HTTP.** La extensión deberá interceptar la petición HTTP del navegador, en cuanto el usuario realice alguna a través del navegador.

**PI_RF2. Deshabilitar extensión.** El usuario podrá deshabilitar la extensión, para que ésta no vigile su actividad en el navegador.

**PI_RF3. Habilitar extensión.** El usuario podrá habilitar la extensión, para que ésta vigile constantemente cuando éste realice una petición HTTP.

**Requerimientos no Funcionales.**

**PI_RNF1. Plataforma de implementación.** La extensión será implementada en el navegador Google Chrome.

**PI_RNF2. Versión del navegador** La extensión funcionará a partir de la versión 65.0.3325.181.

**PI_RNF3. Tecnologías para la interfaz de usuario** Para el sistema se hará uso de HTML, JavaScript, CSS, JSON.
[1]

### 3.1.4. Reglas del negocio.

**PI_RN1. Confidencialidad de la actividad web.** En cuando el cliente lo indique por medio de la IU, la extensión deberá dejar de vigilar la actividad que el usuario realice en el navegador. De igual forma, si el usuario indicara dejar de vigilar la actividad web, la extensión así lo hará.

[1] Checar si es necesario especificar que debe estar habilitado JavaScript y si sería Funcional o No funcional

# 4. Desarrollo.

## 4.1. Prototipo I.

### 4.1.1. Diagrama de casos de uso.

Diagrama de casos de uso general para el prototipo I.

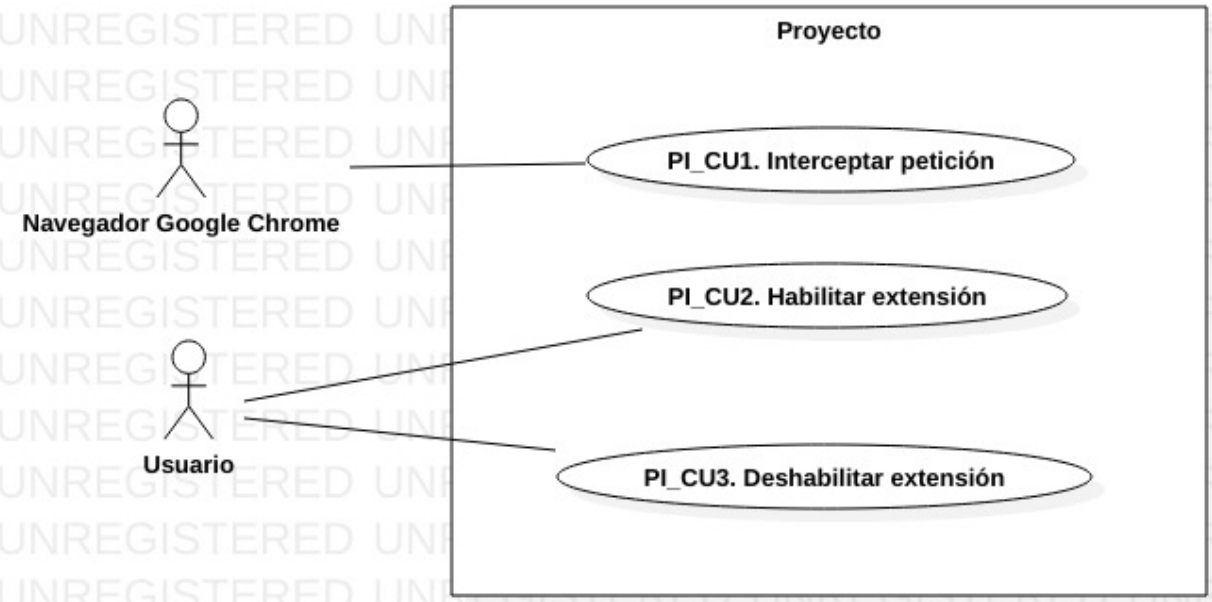


Figura 1: Diagrama de casos de uso.

### 4.1.2. Descripción de casos de uso.

| Caso de uso: PI_CU1. Interceptar petición. | |
|---|---|
| Concepto | Descripción |
| Actor | Navegador de Google Chrome. |
| Propósito | Este caso de uso permite a la extensión interceptar una petición HTTP, realizada por el navegador Google Chrome por medio de algún agente (sistema o usuario) externo a éste. |
| Entradas | Petición HTTP realizada por el navegador. |
| Salidas | Petición HTTP cachada. |
| Pre-condiciones | Algún agente externo (Sistema o usuario) ha ordenado al navegador mandar una petición HTTP. |
| Post-condiciones | La extensión, deberá de interceptar la petición para poder modificarla. |
| Reglas del negocio | - |
| Errores | La petición no se pudo interceptar.<br>La petición no es tipo HTTP. |

Cuadro 5: Descripción CU: PI_CU1

**... Trayectoria Principal ...**

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

2. ***La Extensión*** intercepta la petición antes de que salga a red.

3. ***La Extensión*** puede modificar el contenido de la petición.

4. ***La Extensión*** deja salir a red la petición.

**... Fin de la Trayectoria Principal ...**

**... Trayectoria Alternativa 1 ...**

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

2. ***La Extensión*** ignora la petición.

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

**... Trayectoria Alternativa 2 ...**

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

2. ***La Extensión*** no puede interceptar la petición antes de que salga a red.

3. ***La Extensión*** notifica que hubo un error al intentar interceptar la petición.

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

| Caso de uso: PI_CU2. Habilitar extensión. | |
|---|---|
| Concepto | Descripción |
| Actor | Usuario. |
| Propósito | Este caso de uso, permite al usuario habilitar a 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 | Ninguna. |
| Pre-condiciones | El usuario debe de haber instalado la extensión en Google Chrome y haber permitido su ejecución. |
| Post-condiciones | La extensión verá todas las peticiones que realice el navegador. |
| Reglas del negocio | PI_RN1. |
| Errores | No se puede iniciar la vigilancia de la extensión. |

Cuadro 6: Descripción CU: PI_CU2

**... Trayectoria Principal ...**

1. ***El usuario*** da click en el ícono de la extensión **insert icon**.
2. ***El usuario*** da click en el botón **insert button** "Habilitar extensión".
3. ***La extensión*** empieza a vigilar las peticiones que se realicen a través del navegador.

**... Fin de la Trayectoria Principal ...**

**... Trayectoria Alternativa 1 ...**

1. ***El usuario*** da click en el ícono de la extensión **insert icon**.
2. ***El usuario*** da click en el botón **insert button** "Deshabilitar extensión".
3. ***La extensión*** muestra mensaje de error "La extensión ya está deshabilitada".

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

**... Trayectoria Alternativa 2 ...**

1. ***El usuario*** no encuentra el ícono de la extensión **insert icon**.

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

| Caso de uso: PI_CU3. Deshabilitar extensión. | |
|---|---|
| Concepto | Descripción |
| Actor | Usuario. |
| Propósito | Este caso de uso, permite al usuario deshabilitar a 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 | Ninguna. |
| Pre-condiciones | El usuario debe de haber instalado la extensión en Google Chrome y haber permitido su ejecución. |
| Post-condiciones | La extensión dejará de ver todas las peticiones que realice el navegador. |
| Reglas del negocio | PI_RN1. |
| Errores | No se puede detener la vigilancia de la aplicación. |

Cuadro 7: Descripción CU: PI_CU3

**... Trayectoria Principal ...**

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

**... Fin de la Trayectoria Principal ...**

**... Trayectoria Alternativa 1 ...**

1. ***El usuario*** da click en el ícono de la extensión **insert icon**.
2. ***El usuario*** da click en el botón **insert button** "Habilitar extensión".
3. ***La extensión*** muestra mensaje de error "La extensión ya está habilitada".

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

**... Trayectoria Alternativa 2 ...**

1. ***El usuario*** no encuentra el ícono de la extensión **insert icon**.

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

#### 4.1.3. Diagrama de flujo.

#### 4.1.4. Flujo de datos.

#### 4.1.5. Diagrama de clases.

#### 4.1.6. Diagrama de secuencia.

#### 4.1.7. Interfaz de usuario.

#### 4.1.8. Requisitos de diseño.

# Referencias


[1] https://www.dtic.upf.edu/ tnavarrete/fcsig/javascript.pdf

[2] https://norfipc.com/internet/extensiones-mas-utiles-practicas-navegador-google-chrome.html

[3] https://blog.ensalza.com/diccionario/que-es-una-extension-google-chrome