Universidad de Talca
Facultad de Ingeniería
Departamento de Ciencias de la Computación

Seguridad Informática

Laboratorio 2

Erik Regla
eregla09@alumnos.utalca.cl

20 de mayo de 2020

Índice

1. Actividades

1.1. Actividad 1

Instale el cliente de correo Thunderbird según la versión de sistema operativo que posea. Una vez terminada la instalación del cliente de correo, configure su cuenta de correo institucional y haga pruebas de envío y recepción de correo electrónico para comprobar dicha configuración. ¿Durante la instalación y configuración debió aplicar alguna opción o medida de seguridad?

```
#/bin/bash
## Instalación de thunderbird
sudo apt install -y thunderbird
```

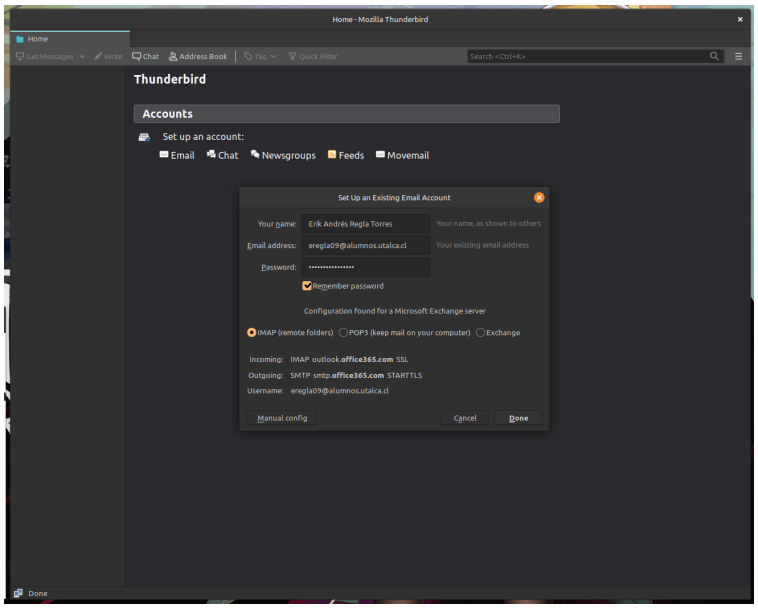

Figura 1: Actividad 1: Instalación de thunderbird

Durante la instalación adicionalmente a la contraseña no fue solicitado ningún otro mecanismo de autenticación.

1.2. Actividad 2

Una vez configurada y probada su cuenta de correo, aplique las siguientes medidas para mejorar la seguridad y uso del cliente de correo: Mostrar cuerpo del mensaje como Texto, Inhabilitar el envío de correo electrónico HTML, Configurar contraseña maestra, No permitir contenido remoto en mensajes, No recordar sitios web y enlaces que haya visitado, No aceptar cookies de los sitios, Permitir a los antivirus poner en cuarentena mensajes individuales. En el informe deberá explicar

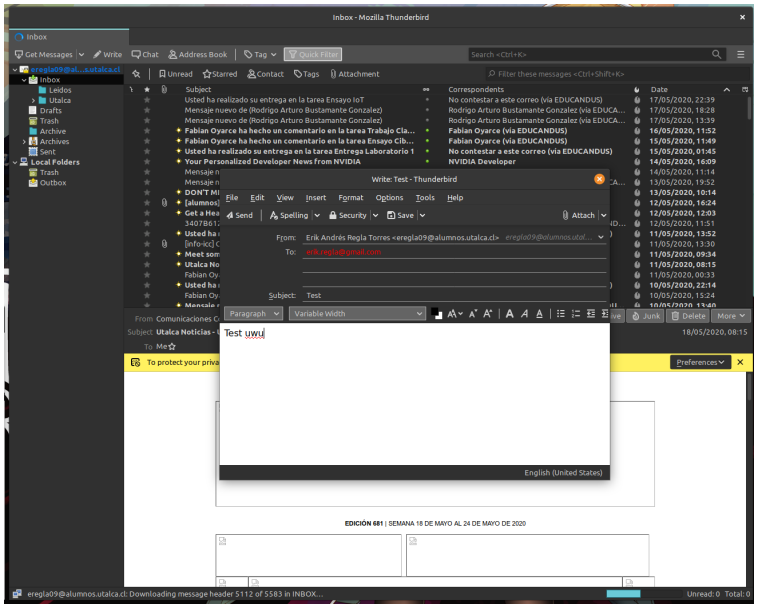

Figura 2: Actividad 1: Instalación de thunderbird

como cada una de las medidas solicitadas ayudan a mejorar la seguridad y cual es la propiedad que ayuda a mejorar (Integridad, Confidencialidad o Integridad).

Efectos en la integridad, confidencialidad y disponibilidad[1]:

- **Mostrar cuerpo del mensaje como Texto:** La visualización del correo se lleva a cabo en navegadores, los cuales podrían contener enlaces maliciosos ocultos dentro de el texto bajo tipografias similares, ejecución de scripts, etc.
- **Inhabilitar el envío de correo electrónico HTML:** Idem a la anterior pero en el caso del envío, a modo de proteger a nuestro destinatario y su disponibilidad del servicio.
- **Configurar contraseña maestra:** Permite almacenar las contraseñas por medio de un llavero, el cual *teoricamente* solo funciona dentro de la misma máquina donde este se creó (en la práctica no es el caso), de este modo evita la escritura manual de contraseñas. Arma de doble filo.
- **No permitir contenido remoto en mensajes:** Permite mantener una lectura confidencial del correo al evitar el uso de trackers como *pixeles*.
- **No recordar sitios web y enlaces que haya visitado:** Previene la obtención de historiales desde el navegador integrado al lector de correo para proteger la confidencialidad del usuario.
- **No aceptar cookies de los sitios:** Idem a la anterior pero con las cookies almacenadas.

[1]La cual está mal escrita en el enunciado

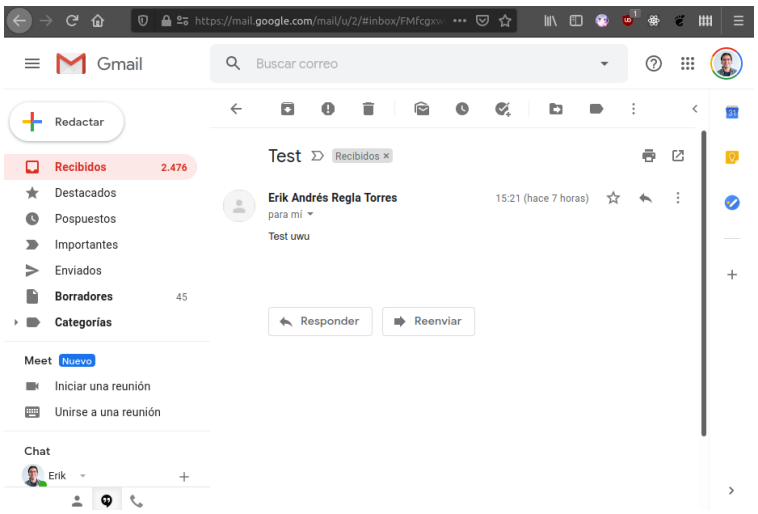

Figura 3: Actividad 1: Lectura de correo enviado a Gmail

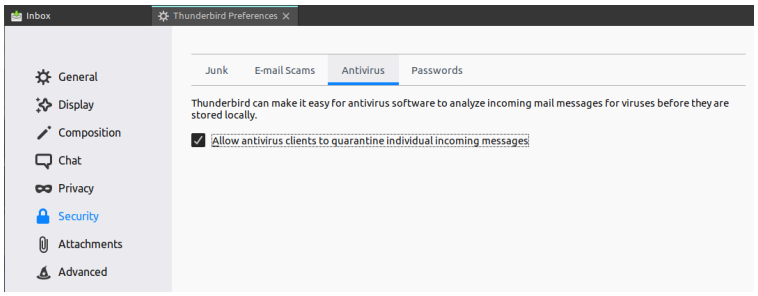

Figura 4: Actividad 2: Configuración de seguridad de ThunderBird

- **Permitir a los antivirus poner en cuarentena mensajes individuales:** En el caso que algun mensaje pueda tener contenido malicioso permite que una heramienta externa pueda aislarlo, protegiendo la disponibilidad de los demás mensajes de manera individual como la de la aplicación (obviamente cubre todos los aspectos y solo funciona si tienes antivirus).

1.3. Actividad 3

Utilice el cliente de correo Thunderbird y el complemento Enigmail para Thunderbird para realizar el envío de correo firmado y cifrado. Utilice la cuenta de correo de alumno para configurar su set de claves y envíe su clave pública a robustamante@utalca.cl. Nota: Necesitará la clave pública del correo robustamante@utalca.cl, la cual deberá solicitar durante la realización de la práctica.

1.4. Actividad 4

Además, deberá investigar qué es y como funciona PGP, dando énfasis en porqué es importante

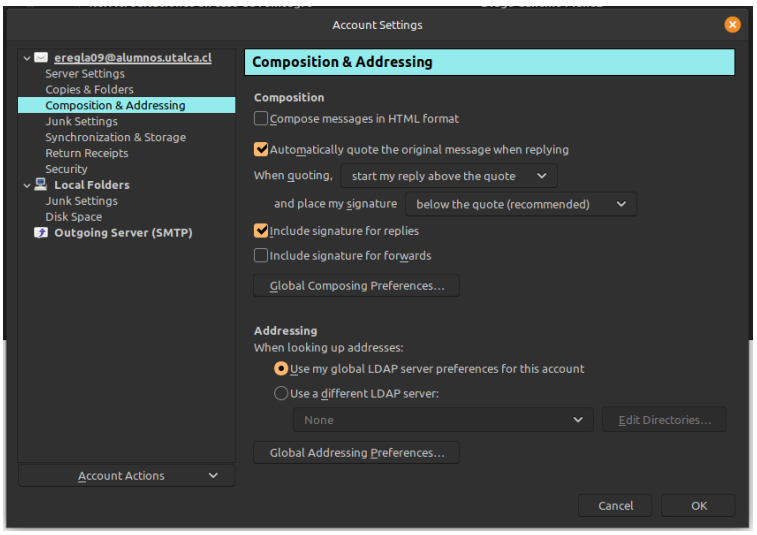

Figura 5: Actividad 2: Configuración de seguridad de ThunderBird

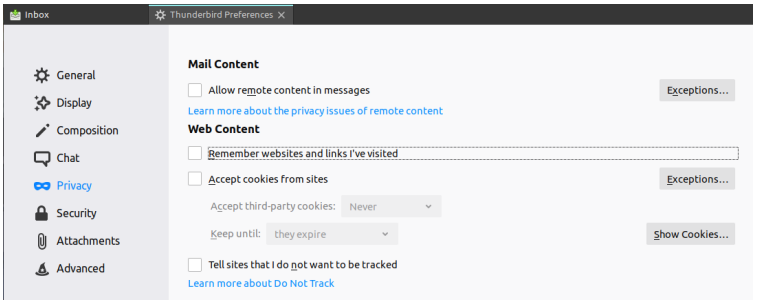

Figura 6: Actividad 2: Configuración de seguridad de ThunderBird

utilizarlo y como piensa que ayuda a la Confidencialidad, Integridad y Disponibilidad.

La encripción PGP se basa en el *protocolo de llave pública*, en la cual cada contraparte contiene fragmentos de la llave del destinatario, permitiendole cifrar el contenido. Una forma de visualizar este proceso es con la analogía del cofre y la llave. Supongamos que deseamos enviar una carta de una persona a otra, pero no queremos que nadie mas lea esta. La condicion inicial es que toda transferencia pasa por un tercero, quien puede leer el mensaje. Entonces, nuestro destinatario nos entrega un cofre abierto (la llave pública) que utilizamos para almacenar nuestra carta y luego cerramos el cofre (cifrado con llave pública). Luego enviamos el cofre el cual nadie es capaz de abrir (ya que nadie tiene la llave) y una vez llega al destinatario este puede abrir el cofre utilizando la llave que solo el posee (llave privada) y leer la carta (leer el mensaje).

Para que este proceso pueda funcionar, es previo necesario intercambiar llaves públicas. ESto ayuda a mantener la confidencialidad del mensaje ya que si la llave pública es capturada por un tercero, su único uso es cifrar mensajes para que los pueda leer un tercero, esta llave per se no es capaz de decriptar información alguna *en teoría*.[1]

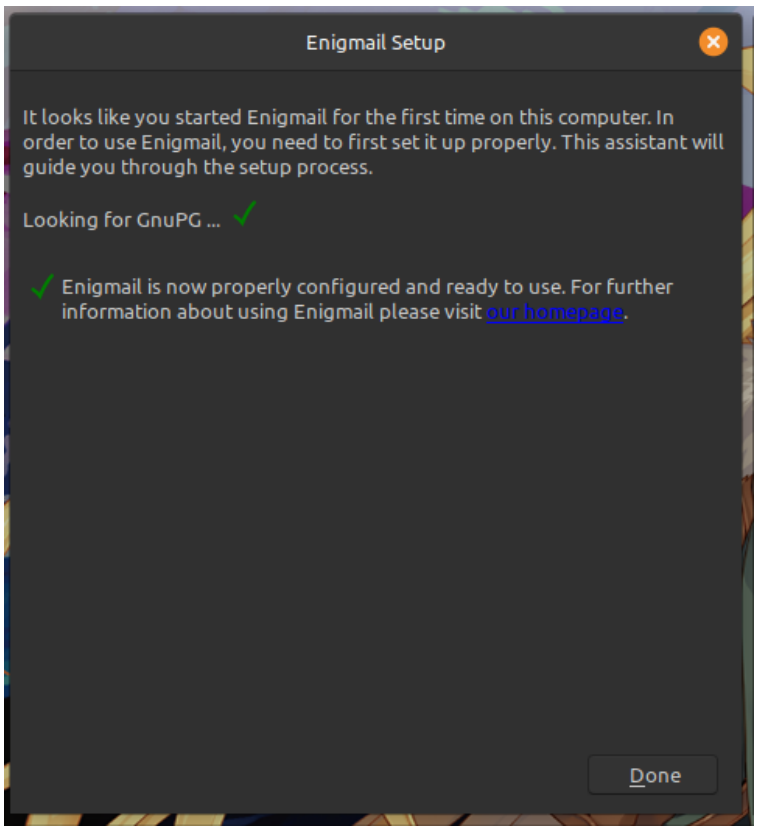

Figura 7: Actividad 3: Envío de llave pública

Sin embargo este método no está libre de vulnerabilidades, como por ejemplo ataques de exfiltración, los cuales abusan del contenido activo de un documento HTML para poder exfiltrar contenido por medio de los enlaces que este puede contener[2]. Sin embargo este tipo de ataques no afecta directamente a PGP, si no mas bien a los clientes involucrados en el manejo de este y las practicas derivadas del mismo. No es como si fuera a ser final de PGP[3].

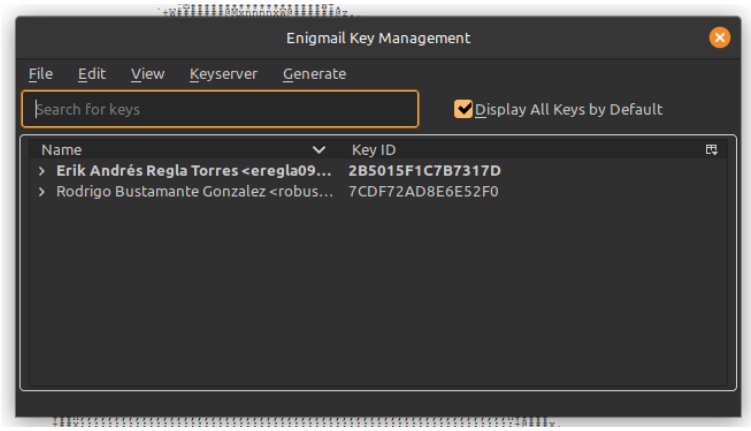

Figura 8: Actividad 3: Envío de llave pública

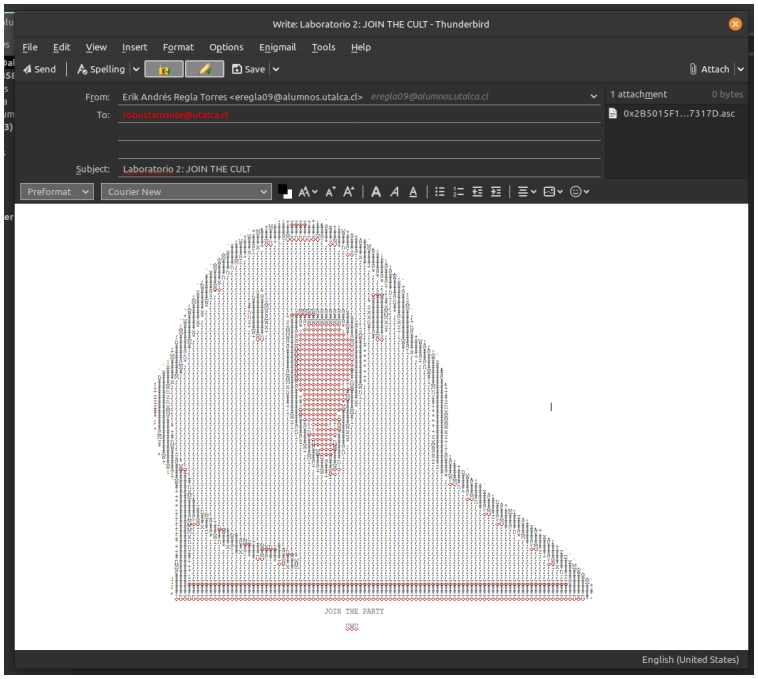

Figura 9: Actividad 3: Envío de llave pública

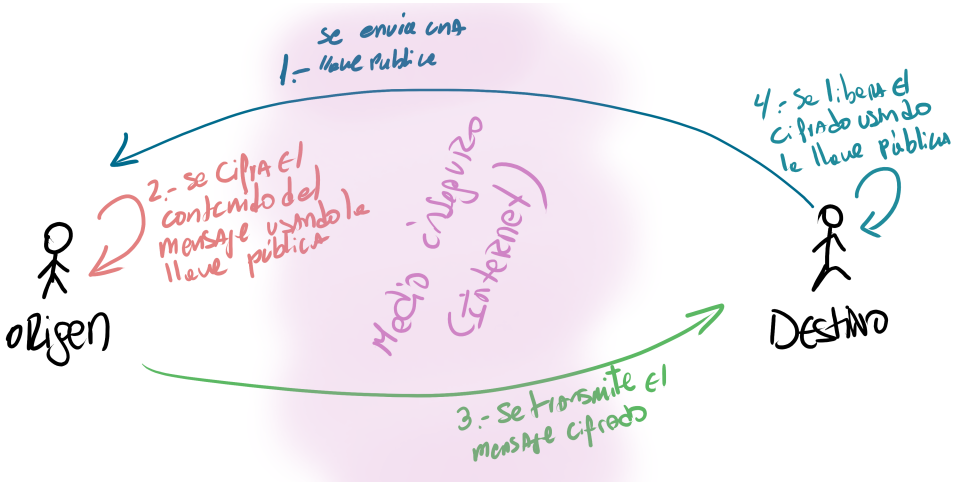

Figura 10: Actividad 4: Caricaturización de como funciona PGP

Referencias

[1] GnuPG Homepage. *Documentation*. https://gnupg.org/faq/gnupg-faq.html.

[2] eFail.de Homepage. *Homepage*. https://efail.de.

[3] Hackaday. *Explaining Efail And Why It Isn't The End Of Email Privacy*. https://hackaday.com/2018/05/21/explaining-efail-and-why-it-isnt-the-end-of-email-privacy/.