Marco teórico.

Para poder abordar mejor la problemática descrita en este documento daremos a continuación una breve explicación sobre los conceptos que ocuparemos durante todo el desarrollo del tema. Esto ayudara al lector a que tenga una mejor apreciación del problema que se desea resolver y a su vez tenga las bases suficientes para vislumbrar cual es que se plantea para resolver nuestra problemática.

Para poder definir el problema que queremos abordar necesitamos definir una de las tecnologías más ocupadas en el mundo y también fue uno de los primeros servicios que se crearon en los inicios del internet para comunicar a sus usuarios entre sí.

1.-Correo electrónico.

El correo electrónico es el servicio por el cual se pueden enviar mensajes entre 2 usuarios que cuenten con este servicio. En sus inicios este servicio solo enviaba texto, pero al pasar de los años hay tenido que soportar el envió de archivos y elementos multimedia.

Para poder enviar un mensaje de correo electrónico es necesario tener ciertos elementos básicos como son:

- Dirección del remitente: Esta dirección se compone por dos elementos importantes, el primero es el nombre de usuario seguido de un carácter “@”, el segundo elemento es el dominio donde está alojado el servicio de correo electrónico.

- Direcciones de los receptores: En un correo electrónico debe haber al menos una dirección de receptor para ser enviado, esta dirección de receptor tiene la misma estructura que la dirección del remitente.

- Contenido del mensaje: Es el texto que se desea transmitir entre el remitente y el receptor.

El mensaje de correo electrónico cuenta con más elementos pero estos son opcionales y se pueden consultar en el RFC 2821 extensión MIME.

El servicio de correo electrónico es proporcionado por un servidor en algún lugar del internet o en la intranet si es que el servicio de correos es privado, este servidor está asignado a un dominio y es un software que se encarga de administrar las peticiones que hacer los usuarios de correo electrónico que tiene registrados.

2.-Servidor de correo.
Un servidor de correo es un programa que se encarga de enviar y recibir los mensajes de correo electrónicos de sus usuarios registrados, este servidor puede recibir mensajes de usuarios de otros servidores de correos que sean dirigidos a sus usuarios registrados.

Este servidor tiene que seguir algunos protocolos que existen en internet para él envió de mensajes de correo electrónico (protocolo smtp) y recepción de mensajes de correo electrónico (protocolo pop3 o imap).

3.-Protocolo SMTP

El protocolo SMTP significa “protocolo para transferencia simple de correo” o “Simple Mail Transfer Protocol” por sus siglas en inglés, el cual se encarga de enviar los mensajes de correo electrónicos entre dispositivos que se encuentran interconectados en la red o en internet. Este protocolo nos ayuda a mandar los mensajes entre 2 usuarios de servidores diferentes, Este protocolo solo se utiliza para mandar los mensajes entre servidores o entre el remitente el usuario emisor y su servidor de correo electrónico.

Este protocolo tiene algunas deficiencia, por lo consiguiente se auxilia de otros 2 protocolos para hacer la transferencia de los mensajes entre el remitente y su servidor de correos. Los protocolos son POP3 y IMAP.

1. Protocolo POP3.

   Este protocolo se encarga de descargar los mensajes del servidor a un cliente de correo electrónico que el usuario haya configurado previamente. Este protocolo solo se sincroniza para la descarga de los mensajes de correo y no deja una copia de seguridad en el servidor de correo electrónico. Este protocolo se puede consultar en el RFC 1939

2. Protocolo IMAP

   Este protocolo, al igual que el protocolo POP3, se encarga de la descarga de los mensajes del servidor a un cliente de correo electrónico con la diferencia de que la sincronizacion entre el servidor de correos electronico y el cliente de correos es continua y se mantiene una copia de seguridad en el servidor. Con este protocolo es posible tener varios clientes de correo configurados con la misma cuenta y los cambios que se realicen en cualquiera de los clientes de correo se verá reflejado en el servidor y en los diferentes clientes sincronizados. Este protocolo puede ser consultado en el RFC 6851.

5.-Clientes de correo (Tipos)
6.-Amenazas
7.-Algoritmos y esquemas de cifrado (sincono y asincono)
8.-Agentes Clasificadores

Estado del Arte

La unica referencia que tenemos sobre un esquema criptografico contra adversarios clasificadores es el que encontramos en el articulo “Defending Email Communication Against Profiling Attacks” de Philippe Golle y Ayman Farahat, ambos miembros del “Palo Alto Research Center”.
En su artículo aborda el tema del ataque de los adversarios clasificadores proponiendo un esquema de cifrado simple de llave simétrica en el cual la llava que se usa para cifrar esta dada por la cabecera del correo electrónico (que consiste en la dirección del remitente, la dirección del destinatario, la hora a la que se envía el correo electrónico y potencialmente otros campos). Esto le permite al destinatario calcular la llave facilmente ya que estos datos son publicos, este esquema es inseguro contra un adversario normal, pero es seguro contra adversarios

clasificadores, ya que los clasificadores al procesar la información por volumen si quisieran descifrar el contenido del correo tardarian en descifrar todos por la gran cantidad de correos que procesan en cada lote.

10.-Propuesta (Esquema y Acotacion)

1.-Esquema
2.-PGP
3.-CAPTCHA

4.-SSE.
5.-Tecnologias.
    1.-Cifrado
    2.-Tablas HASH
    3.-Generadores de CAPTCHAS
    4.-Servicores
    5.-Protocolos
    6.-S.O.
    7.-Clientes de Correos
    8.-Lenguajes de Programacion

Referencia

[6] Trend Micro, “Email encryption”, Internet: http://www.trendmicro.es/productos/email-encryption/

[7] Office, “Cifrar mensaje de correo electrónico”, Internet: https://support.office.com/es-es/article/Cifrar-mensajes-de-correo-electr%C3%B3nico-84d7e382-5f76-4d71-8705-324489b710a2?CorrelationId=d5c846d3-8fb7-4935-b67e-6548a430acd4&ui=es-ES&rs=es-ES&ad=ES

[8] Mailvelope, “Documentation”, Internet: https://www.mailvelope.com/help

[9] Thunderbird, “Firma digital y cifrado de mensajes”, Internet: https://support.mozilla.org/es/kb/firma-digital-y-cifrado-de-mensajes

[10] OPTENET Get Optimal Internet, “Clasificación de texto con adversario Técnicas de clasificación y filtrado aplicadas a la detección de spam en la Web”, Internet: http://www.esi.uem.es/jmgomez/papers/soria08.pdf