

Centro Universitario de Ciencias Exactas e Ingenierías.
Departamento de Ciencias Computacionales.



Materia:

Sistemas Operativos.

Profesora:

Becerra Velázquez Violeta del Rocío.

Alumno:

Maldonado Melendez Diego Alberto.

Código:

221977845.

Carrera:

Ingeniería en Computación.

Sección:

D04

Título del ensayo:

La seguridad de nuestra información.

Fecha:

29 de noviembre de 2023.

La evolución de nuestra raza ha provocado que la humanidad busque cada vez más privacidad. Desde la cantidad de dinero que tenemos en una cuenta de banco, hasta una idea con la que podemos lucrar y no queremos que otro se aproveche, toda esa información es de gran valía, y requiere ser resguardada. De igual manera, y gracias al surgimiento del mundo digital, la información de los individuos ha migrado a cada uno de los dispositivos que utilice, por lo que ya no solo es labor del usuario protegerla, sino también de las redes y los sistemas con los que pueda interactuar.

Esto hace que salvaguardar la seguridad de la información de los usuarios sea algo más complejo y abstracto, esto debido a que una persona sin conocimientos informáticos puede no saber cómo funcionan las redes y los sistemas operativos. Afortunadamente ha habido personas y organizaciones que se han encargado de desarrollar métodos capaces de lograr este cometido.

Uno de estos métodos es conocido como criptografía. Este término lleva presente en la sociedad desde hace siglos. Según la Real Academia Española, criptografía hace referencia al “arte de escribir con clave secreta o de un modo enigmático”. En una primera instancia, civilizaciones antiguas empleaban la criptografía para comunicarse sin ser cifrados por comunidades enemigas. Trasladado a un área más contemporánea, según la Universidad Internacional de Valencia (2021), la criptografía “protege los sistemas informáticos y de tecnología de la información mediante la creación de algoritmos y códigos para cifrar los datos”.

La etimología puede decir mucho sobre algo. Previo a este trabajo, desconocía que existía relación entre la criptografía y la informática, a pesar de constantemente enfrentarme a cifrado de datos, protocolos de seguridad, entre otras situaciones que se basan en la encriptación de información. Considero a la criptografía como un elemento crucial para la protección de nuestros datos. En el caso de los sistemas operativos, es el escudo que impide que los datos que yacen en el disco sean burlados. En las redes, por otro lado, permite que una comunicación entre dispositivos se realice de manera satisfactoria, sin que la información sea interceptada.

La esteganografía, al igual que la criptografía, se basa en el cifrado de la información para ser transmitida de manera segura. Una excelente analogía de su funcionamiento es el famoso caballo de Troya. A diferencia de la criptografía, la esteganografía busca hacer ver que no existe ningún mensaje, disfrazándolo de otro tipo de dato que no tiene inconveniente en ser mostrado. No obstante, el fin es el mismo, esconder información relevante dentro de elementos como los ficheros. Su uso en redes es un poco abstracto, pero se basa en la idea de que la información pase inadvertida a la hora de enfrentarse a sistemas de detección.

Todo parece color de rosas hasta el momento. No obstante, ¿son realmente necesarias estas herramientas para la protección? Y más importante aún, ¿logran su cometido? Según información proporcionada por la empresa Symantec, en el año 2019 se detectaron alrededor de 5 mil millones de amenazas. Además, en una encuesta realizada por la misma compañía, el 94% de las personas no se siente cómoda con la carga de trabajo e información que tienen en la nube.

Otro ejemplo es que, en 2016, se comprometieron mil millones de registros de datos, información obtenida gracias a un informe de la empresa Gemalto. Contrarrestando a esto, y según el Reporte de transparencia de Google, el 11 de noviembre de este año, el 95% de las búsquedas realizadas en esta herramienta fueron mediante el protocolo de seguridad HTTPS, técnica criptográfica, y como este protocolo hay otros como TCP, UDP, IPv4 e IPv6, que todos, en conjunto, buscan que la información se transmita correctamente desde y hacia dónde desee el usuario. Pero a pesar de ellos, las redes en general, y las públicas en particular, siguen teniendo lagunas en las que pueden ingresar los atacantes y burlar vulnerabilidades.

Como podemos observar, existe la suficiente cantidad de ataques cibernéticos para requerir de técnicas capaces de contrarrestarlos. No obstante, lo que considero el punto más importante de todo esto es que, incluso teniendo cierto acercamiento a la informática y al funcionamiento de los sistemas y leyes, no podemos tener una certeza de cómo se mueven nuestros datos en el mundo digital. Por ejemplo, a la hora de utilizar internet, estamos a expensas de lo que decidan hacer las empresas con nuestros datos en sus servidores, y una vez algo sale de nuestra posesión, es complicado saber en dónde pueden recabar.

Es por ello por lo que, a pesar de que la ciberseguridad ha llegado a un punto muy avanzado, en donde existen sistemas, algoritmos y técnicas que ayudan a que nuestra información esté un poco más segura, también influye mucho el comportamiento y la consciencia de las personas a la hora de introducirse en el mundo digital. Por ejemplo, muchos pensamos que no hay ningún inconveniente con ver películas en páginas no oficiales y que incentivan la piratería. Esto hace que haya posibilidades de que nuestra información se vea comprometida y, por consiguiente, sufrir de algún ataque cibernético.

Un trabajo en conjunto entre las técnicas para la encriptación de datos, como la criptografía y esteganografía, y un uso consciente de dispositivos electrónicos, permitirá que la información de los usuarios esté más segura, y la posibilidad de ataques disminuya. Las técnicas mencionadas son el producto de un extenso esfuerzo humano en idear maneras de transmitir información con la certeza de que alguien no deseado la lea. Por otro lado, el usuario puede atañerse a técnicas simples pero efectivas, como evitar usar la misma contraseña en muchas plataformas, usar contraseñas seguras, y leer los términos y condiciones, siendo esto último algo tedioso, pero que considero necesario para saber cómo serán tratados nuestros datos.

Por todo lo anteriormente expuesto, se exhorta a los usuarios a tener una buena complementación entre técnicas para la codificación y encriptación de la información, junto con buenas prácticas de seguridad digital. Para las técnicas de seguridad destacar la criptografía y esteganografía, ambas basadas en transmitir una información de forma que no parezca lo que en realidad es, pero la primera de ambas busca encriptar dichos datos, mientras que la segunda se basa en esconder dichos datos en algún otro elemento. Pero lo más importante de todo es que los usuarios tengan consciencia de lo que es la huella digital, que una vez que algo está en la nube es complicado eliminarlo, y que no tenemos completo control sobre nuestra información en el mundo digital, por lo que hay que ser cuidadosos en todo momento, para así poder disfrutar de las ventajas que nos ofrece la tecnología.

Referencias.

González, A. (2021). Esteganografía. Definición, técnicas y usos frecuentes. *Ayuda Ley*

Protección Datos. <https://ayudaleyprotecciondatos.es/2021/03/17/esteganografia/>

Haley, K. (2019, 12 julio). El Informe sobre amenazas de seguridad en la nube de Symantec

CSTR 2019. *Symantec Enterprise Blogs*. [https://symantec-enterprise-](https://symantec-enterprise-blogs.security.com/blogs/america-latina/informe-de-amenazas-de-seguridad-en-la-nube)

[blogs.security.com/blogs/america-latina/informe-de-amenazas-de-seguridad-en-la-nube](https://symantec-enterprise-blogs.security.com/blogs/america-latina/informe-de-amenazas-de-seguridad-en-la-nube)

Universidad Internacional de Valencia. (2021). Qué es la criptografía y cuáles son sus usos.

VIU España. <https://www.universidadviu.com/es/actualidad/nuestros-expertos/que-es-la-criptografia-y-cuales-son-sus-usos#>