

Sistema informático para la detección de activación de cámara o micrófono de un equipo de cómputo.

Trabajo Terminal No. _____ - _____

Alumnos: Guerra García Eliel Josué y Santos Cortés Nataly

Directores: Dr. Tonáhtiu Arturo Ramírez Romero,

**e-mail: eguerra1500@alumno.ipn.mx*

Resumen: Se realizará un sistema informático que ayude a mantener la privacidad de cualquier usuario a la hora de trabajar en su equipo de cómputo. Este sistema será capaz de poder brindar información oportuna para dar conocimiento a el usuario de que se está vulnerando su privacidad principalmente la detección de acciones como la activación de cámara o micrófono de su equipo de cómputo para que el usuario tome medidas oportunas.

Palabras clave: Ciberseguridad, Espionaje, Privacidad y Redes

1.Introducción

Con la evolución acelerada de la tecnología a lo largo del siglo XXI y con la notable creciente del internet el Marketing Digital ha venido a evolucionar la forma de venta, las herramientas que la integran logran influir sobre determinado grupo de posibles consumidores, a fin de captarlos para que compren algún producto o servicio y aunque el marketing digital ha democratizado la promoción también sus herramientas han sido motivo de preocupación no solo porque interpretan y almacenan nuestro comportamiento sino porque podrían cruzar la delicada línea de la privacidad.

Es de dominio público que existen intereses militares, políticos y comerciales a nivel mundial y este último conlleva a un innegable riesgo de que la privacidad de los usuarios esté comprometida para fines comerciales, los piratas informáticos realizan las principales filtraciones, que mediante software malicioso acceden y roban información sensible, producen daños en los equipos, entre muchas otras actividades ilegales.

Diferentes experimentos realizados como el de la docente e investigadora mexicana [1] pueden verificar que a las herramientas de marketing digital ya no le es suficiente al espiar tu historial para ofrecerle publicidad relacionada, sino que sus metodologías han trascendido a intervenir llamadas telefónicas, mensajes de Whatsapp o Telegram, mensaje de voz y lo que resulta muy preocupante hablando en vivo con el celular a un lado, sin uso.

Sistemas similares que se han desarrollado son.

1. Función de privacidad de iOS 14
2. Access Safe Dots
3. Kaspersky Lab

Software	Características	Precio en el Mercado
iOS 14	Activa Reporte de Privacidad de Apps y descubre de un vistazo lo que han estado haciendo tus apps. En una sección de Configuración, verás con qué frecuencia han accedido a tu ubicación, fotos, cámara, micrófono y contactos en los últimos siete días. [4]	Tener un dispositivo APPLE que soporte el sistema operativo iOS 14 o superior
Access Safe Dots	Al presentar Access Safe Dots, agrega los mismos indicadores de estilo iOS 14 (algunos píxeles se iluminan como un punto) en la esquina superior derecha (predeterminada) de su pantalla cada vez que cualquier aplicación o servicio de terceros usa la cámara o el micrófono de su teléfono.[5]	Gratuito
Kaspersky Lab	la cual advierte a los usuarios si su información privada está siendo monitoreada por algún spyware o software espía ofrecido comercialmente. Aunque este tipo de software se considera legal, la presencia del programa es a menudo tan indeseada como desconocida por el usuario afectado.[6]	<ul style="list-style-type: none"> ● KasperskyAnti-Virus: \$439.20 ● KasperskyInternet Security: \$639.20 ● KasperskyTotal Security: \$499.50 ● KasperskySecurity Cloud Personal: \$679.60

2. Objetivos

Objetivo general:

Desarrollar un sistema que detecte la activación de la cámara y micrófono, que permita brindar al usuario información sobre qué acción se realizó.

Objetivos específicos:

1. Analizar los aspectos relacionados con la seguridad computacional relativa a la cámara y el micrófono.
2. Desarrollar un módulo de monitoreo del estado del micrófono y de la cámara.
3. Desarrollar un módulo de informe del encendido de la cámara o micrófono.
4. Desarrollar un reporte técnico.

3. Justificación

Sin duda alguna Google se ha convertido en parte fundamental y hasta cierto punto valioso por todas las funcionalidades que tiene y servicios que brinda esto ha provocado que sus usuarios brinden información personal y sensible, pero siendo una empresa transnacional da cierta seguridad que la tenga en su poder e inclusive que te monitoreen para poder brindar un mejor servicio, el hecho de pensar que su seguridad sea vulnerada se visualiza casi imposible.

Google permite configurar la privacidad de tu cuenta para restringir cierto tipo de servicios [2]. El hablar de sustituirla sería algo muy radical por todo lo que ofrece más sin embargo se considera fundamental que el usuario tenga la certeza de que va a ser monitoreado y evitar ponernos en situaciones que no queramos ya con el conocimiento anticipado esto implica no decir o hacer en la red algo que pueda comprometernos o meternos en problemas. No así lo mismo para otros servicios a los cuales la mayoría de las personas desconoce que son monitoreados.

Hoy en día es verdad de que los antivirus ofrecen características bien definidas para poder protegerse de diferentes malware o ataques pero también a su vez hay muchos que entre sus configuraciones son pasadas por alto tipo de virus como spyware y dan permisos no justificados o que comparte imagen y video con terceros sin el conocimiento de los usuarios.

Los riesgos de que nuestra privacidad se vea comprometida son altos en la actualidad, y muchas veces el usuario toma una actitud de dar por sentado que alguien podría estar escuchando lo que se dice, escribe y hace en Internet pero lo que se busca es brindar certeza absoluta al usuario de en qué momento se encuentra monitoreado y por quién.

4. Productos o resultados esperados

1. Un software que haga la detección de la activación de la cámara y micrófono.
2. La documentación técnica del sistema.

5. Metodología

Para el desarrollo de este proyecto se utilizará el modelo de cascada; ya que se tendría una clara comunicación y pasos muy claros; se realizará un análisis en el cual se obtendrán los requisitos específicos que se necesitan y se empezará a realizar el diseño una vez esto, se realizará el código, esta metodología se tiene que realizar por completo un proceso para que llevemos a cabo el siguiente y por último haremos pruebas en diferentes equipos de cómputo.



Figura 1. Fases de la Metodología en Cascada. [3]

Cronograma

CRONOGRAMA Guerra García Eliel Josué

Actividades	A G O	S E P	O C T	N O V	DIC	E N E	FEB	MAR	ABR	MAY	JUN
1. Planteamiento del problema											
2.Investigación											
Investigación de los recursos tecnológicos a utilizar											
3.Análisis											
Elección del entorno de programación											
Análisis de requerimientos del sistema											
4.Diseño											
Diseño de las interfaces del sistema											
Evaluación de Trabajo Terminal I											
5. Desarrollo											
Codificación de las interfaces del sistema											
Pruebas y modificaciones.											
6. Documentación											
Manual de usuario											
Casos de uso											
Manual técnico											
Evaluación de Trabajo Terminal II											

CRONOGRAMA Santos Cortes Nataly[illegible]

7. Referencias

- [1] R. Torres, "*Experimento de publicidad*", *Twitter*, 2021. [En línea]. Disponible en: https://twitter.com/Rql_Torres/status/1368298464296247296?s=20 (accedido el 16 de abril de 2021)
- [2] A. Borjas. "Cómo evitar que Google escuche y me espíen". *islaBit*, 2020. [En línea]. Disponible en: <https://www.islabit.com/107868/como-evitar-que-google-escuche-y-me-espian.html> (accedido el 16 de abril de 2022).
- [3] S. Laoyan. "Todo lo que necesitas saber acerca de la gestión de proyectos en cascada". *Asana*, 2021.[En línea]. Disponible en: <https://asana.com/es/resources/waterfall-project-management-methodology> (accedido el 16 de abril de 2022).
- [4] "Access Safe Dots : Access Indicator para PC". *APPPARAPC.com*, 2022 <https://appparapc.com/apk/9327208/> (accedido el 27 de abril de 2022).
- [5] "Tú decides lo que quieres compartir". *Apple*, 2021. <https://www.apple.com/mx/privacy/control/> (accedido el 27 de abril de 2022).
- [6] "Kaspersky Lab habilita alerta de privacidad contra el spyware para móviles". *Kaspersky*. https://latam.kaspersky.com/about/press-releases/2019_kaspersky-lab-habilita-alerta-de-privacidad-contra-el-spyware-para-m-viles (accedido el 27 de abril de 2022).

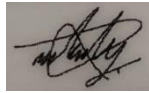
8. Alumnos y Directores

Guerra García Eliel Josue.- Alumno de la carrera de Ing. en Sistemas Computacionales en ESCOM, Especialidad Sistemas, Boleta:2019630232 , Tel. 5539143119 , email: eguerra1500@alumno.ipn.mx



Firma: _____

Santos Cortés Nataly.- Alumna de la carrera de Ing. en Sistemas Computacionales en ESCOM, Especialidad Sistemas, Boleta:2019630038 , Tel. 5575200535 , email: nsantos1800@alumno.ipn.mx



Firma: _____

Dr. Tonáhtiu Arturo Ramírez Romero.- Doctor en ingeniería de sistemas, profesor investigador. Áreas de interés: Inteligencia artificial, bases de datos, desarrollo de sistemas web y sistemas complejos. Publicaciones en congresos nacionales e internacionales, así como en revistas científicas arbitradas. Departamento de Ciencias e Ingeniería de la Computación, Escuela Superior de Cómputo, Tel. 57296000, ext. 52052. email: *tonahtiu@yahoo.com*

Firma: _____



CARÁCTER: Confidencial

FUNDAMENTO LEGAL: Artículo 11 Fracc. V, Artículos 108, 113 y 117 de la Ley Federal de Transparencia y Acceso a la Información Pública

PARTES CONFIDENCIALES: Número de boleta y teléfono