un documento filtrado a la prensa muestra como España se posiciona ante Europa como el mayor defensor de prohibir a empresas europeas el uso de tecnologías de cifrado extremo extremo para combatir el abuso sexual infantil permitiendo el acceso a todas nuestras comunicaciones online un nuevo ataque de canal lateral contraprocesadores de móviles iPhone y Android y portátiles de Apple revela como ciberdelincuentes podrían espiarte a través de los píxeles de tu pantalla y saber qué páginas estás visitando o incluso robar tu identidad online la cuenta atrás avanza y ya estamos a solo cinco episodios de llegar a los 100 Nos acompañas Comencemos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast ubicamos este episodio el 29 de mayo de 2023 es el episodio 95 yo soy Martín vigo y está conmigo con el micrófono ya implantado en su rostro Alexis porros Hola Alexis qué tal me ha recordado a la empresa de nuestro querido elon mus neuralink tengo el micrófono implantado en mis cuerdas vocales quería decir No pues nada muy bien muy bien Martín de nuevo ya haya rutina esto ya ya como como cada semana un episodio nuevo fresco del horno y nada pues para no enrollarme más dar siempre las gracias a nuestros oyentes que episodio tras episodio están con nosotros y bueno darle las gracias también por escucharnos por enviarnos sus sugerencias preguntas inquietudes en todas las plataformas sociales en las que estamos en discord también ahí podéis acceder vía tierra de hackers.com barra discord y bueno lo que he dicho estamos En plataformas sociales como tierra de hackers o como arroba tierra de hackers y también obviamente en las plataformas de podcast donde si no está ya podéis ir ahora mismo a suscribiros para que os llegue la notificación de los próximos podcasts Y como siempre También la el agradecimiento a que votéis a la pregunta del episodio que siempre publicamos en Twitter y que la del episodio anterior fue la siguiente A dónde nos lleva la Inteligencia artificial Teníamos dos respuestas y la más dotada con un 60% fue a un mundo mejor seguida de 40% a un mundo peor Así que parece que no es muy grande la diferencia pero la gente es es optimista con el tema de la Inteligencia artificial Bueno yo no sé si diría que la gente es optimista porque está casi ahí en el Fifty Fifty yo a partir del 80% famosos cuando diría bueno la gente es optimista más sorprendido eh pensaba que la gente a ver yo en general quiero pensar que nos va a llevar a pesar de que como damos las noticias Porque al fin y al cabo hay que cubrir la actualidad Yo quiero pensar que nos va a llevar un mundo mejor no entiendo que ha habido tecnologías que asustaban en muchos periodos de la historia pero bueno sí que sí que tenemos a expertos esta vez alertando no pero bueno yo sería de los que votaría a un mundo mejor tú Alexis Sí sí yo también aunque bueno igual como Tenemos tantos oyentes que siguen el podcast se han asustado tanta noticia que traemos sobre ese tema y Pero bueno no es que queramos hacer cundir el pánico pero en Sí si se hace buen uso de la Inteligencia artificial pues probablemente tengamos un mundo mejor yo creo que lo del Matiz es importante creo que no creo que votaría a nos lleva un mundo mejor si hacemos lo que tenemos que hacer para controlar esto no que no se nos vaya de las manos bueno rápidamente yo dar las gracias a nuestros mecenas de patreon como siempre que hacen este podcast posible que lo estés escuchando gratis así de manera gratuita es en parte Gracias a nuestros mecenas de patreon Así que si tú gustas apoyarnos con todos los beneficios que aparte traen los diferentes formas de apoyarnos en patreon puedes hacerlo en tierra hackers.com/patreon Así que ya sabes Ahí nos puedes apoyar y como siempre nuestros sponsors como Pro que es la herramienta más completa de seguridad en aws empresas de todos los tamaños se apoyan diariamente en brawler pro para que sus equipos puedan confiar en su modelo de seguridad de aws puedes probar brawler Pro hoy mismo y de manera totalmente gratuita si obtendrás paneles y gráficas con información concisa y accionable con todo lujo de detalles sobre la madurez de www tu modelo de seguridad y también visión completa de tu infraestructura en todas las regiones de aws y además los resultados los vas a

tener en unos minutos empiezo a usar brawler pro y benefíciate de sus resultados visitando tierra de hackers.com barra brawler Pro prwwerpro y también queremos dar las gracias a otro de nuestros patrocinadores en este caso monat una empresa que comparte los mismos valores que nosotros tierra de hackers hacer la seguridad más accesible y transparente nosotros a través de un podcast y monat con una herramienta de gestión y visualización de telemetría y datos de seguridad fundada en silicon Valley y buscando ingenieros con experiencia en ciberseguridad para ayudarles a construir y hacer realidad su misión contratan en todo el mundo y en remoto así que ya sabéis echadle un vistazo a su web monat.commod.com y mandarles vuestro currículum a tierra de hackers @monat.com Pues venga nos vamos al lío Traigo una noticia que me ha dejado sorprendido y triste a partes iguales una noticia que algunos de vosotros queridos oyentes De hecho ya me pasasteis por discord y por Twitter para que la comentase y eso me encanta porque vosotros mismos decís Oye mírate esto y Cuéntamelo en el podcast Pues aquí estoy voy al grano se ha filtrado un documento a la prensa del Consejo europeo dirigido a las diferentes fuerzas y cuerpos de seguridad de los países miembros en el que se les hace varias preguntas para establecer nuevas regulaciones que facilitan la lucha contra el abuso y explotación sexual infantil el título de dicho documento de hecho es el siguiente propuesta de reglamento del parlamento europeo y del Consejo para establecer normas para prevenir y combatir el abuso sexual infantil bueno el documento que está muy bien estructurado realmente se trata de hacer las cuatro mismas preguntas a cada país miembro de la Unión Europea concretamente a las fuerzas y cuerpos de seguridad y Estas son las cuatro preguntas que contestan la primera pregunta y la más interesante dice lo siguiente Hasta qué punto puede ser afectado el material cifrado de abuso sexual infantil por una orden de detección estás a favor de excluir alguna redacción en el reglamento que excluya el debilitamiento del cifrado De extremo a extremo ver por ejemplo el punto 25 del reglamento 2021 12 32 vale vamos por partes Qué es eso del reglamento europeo 2021 12 32 y cuál es exactamente el punto 25 esto es esencial para entender esta primera pregunta Bueno pues me puse a indagar y busqué la referencia en la web oficial del Consejo europeo que por cierto os dejo las notas del episodio como siempre con la referencias el reglamento europeo 2021 1232 está resumido tal que así reglamento europeo 2021 del parlamento europeo y del Consejo de 14 de julio de 2021 por el que se establece una excepción temporal a determinadas disposiciones de la directiva 2002 58 ce en lo que respecta al uso de tecnologías por proveedores de servicio de comunicaciones interpersonales independientes de la numeración para el el tratamiento de datos personales y de otro tipo con fines de lucha contra los abusos sexuales de menores en línea esto quiere decir que este reglamento pone excepciones a la hora de las leyes que velan por nuestra por defender nuestra privacidad concretamente la de las comunicaciones es decir hay leyes que prohíben a empresas a gobiernos digamos monitorizar nuestras comunicaciones pues este reglamento pone ciertas excepciones concretamente para luchar contra la pornografía infantil Ok Qué dice exactamente el punto 25 de este reglamento cito textualmente el cifrado De extremo a extremo es un instrumento importante para garantizar la seguridad y la confidencialidad de las comunicaciones de los usuarios incluidas las de los menores todo debilitamiento del cifrado puede ser aprovechado por terceros malintencionados quedaos con esto Esto es lo que dice el propio reglamento por tanto ninguna disposición del presente reglamento debe interpretarse en el sentido de que prohíbe o debilita el cifrado de extrema extremo es decir tal como está escrito aquí no se puede tocar el cifrado extremo extremo como me tuve que leer todo el reglamento para preparar esta noticia destaco también el punto 26 que dice lo siguiente el derecho al respeto de la vida privada y familiar incluida la confidencialidad de las comunicaciones es un derecho fundamental garantizado por el artículo 7 de la Carta Magna por tanto también es una

condición necesaria para que haya comunicaciones seguras entre las víctimas de abuso sexuales de menores y un adulto de confianza o de las organizaciones que se dedican a la lucha contra los abusos sexuales de menores y comunicaciones entre las víctimas y sus abogados Entonces nos tenemos que ir ahora que fue lo que hice yo a la Carta Magna que es un poco ese documento histórico que es la base fundamental de la de los derechos de los seres humanos y el artículo 7 dice lo siguiente es inviolable la libertad de difundir opiniones información e ideas a través de cualquier medio básicamente la libertad de expresión OK ahora que entendemos esto y volviendo a la pregunta que que la primera pregunta de esas cuatro que se le plantea a todos los países básicamente está preguntando si deberían excluir el cifrado extremo a extremo del reglamento que añade excepciones al derecho a la privacidad que tenemos sobre nuestras comunicaciones o bueno dicho de otra manera ya que está jerga legal cuesta tampoco está bastante entenderla pregunta si como parte de la excepción que quieren incluir a las leyes que protegen nuestra privacidad deberían omitir el cifrado extremo a extremo para que las excepciones no apliquen en ese caso y se mantenga esa excepción en ese caso es decir básicamente eliminamos el cifrado extremo extremo o no Porque si lo eliminamos así las empresas podrían acceder descifrar digamos nuestras Comunicaciones y por tanto teóricamente Buscar indicios de pornografía infantil Ok segunda pregunta estás a favor de explorar si se debe continuar con las detección voluntaria en caso afirmativo preferirías prolongar el reglamento temporal 2021 1232 o incluir Su contenido en la propuesta del csa la propuesta del csa es básicamente esta propuesta que quieren hacer Esto hace referencia a que ahora mismo las empresas pueden reportar material sospechoso relacionado al abuso sexual a menores a las si así lo desean Como por ejemplo cómo hace Apple al escanear tus fotos de iCloud no buscando esos hashes de la lista de hashes que suele dar Interpol y europol que que saben que es referente a fotografías o material de abuso infantil o la polémica de hace un año más o menos que de hecho cubrimos aquí en el podcast de que Apple iba de hecho empezar a escanear no solo en iCloud que sería sus propios servidores sino en tu propio teléfono no lo cual pues ya es diferente sobre todo legalmente porque ahora ya no escaneas cuando yo subo algo a tu servidor ahora estás escandando mi teléfono la cuestión es si debería seguir permitiendo esa empresa hacer esto o no y puntualizar aquí que esto no quiere decir que lo puedan hacer si tus datos están cifrado a extremo a extremo O sea si está cerrado extremo extremo por mucho que quiera Apple o quien sea no podría vale la siguiente la tercera pregunta que le hacen es estás a favor de incluir las comunicaciones de audio en el ámbito de la propuesta de csa O prefieres excluirlo como se hizo en el reglamento 2021 12 32 esta pregunta concretamente se refiere a que si se debería incluir el audio de las conversaciones O sea no solo el texto de los mensajes como parte del nuevo reglamento lo que significaría que las empresas tendrían acceso a escuchar nuestras conversaciones o si por lo contrario deberíamos excluir el audio del todo y así hacer que las empresas solo pudieran acceder a los mensajes es un poco como si te pones en el ejemplo de WhatsApp pues podrían acceder a la mensajería lo que escribes pero no cuando llamas por teléfono no vale última pregunta con el objetivo de detectar el abuso sexual infantil deseas que la detección se realice en las comunicaciones interpersonales y en el contenido de acceso público o que se limite únicamente al contenido de acceso público esta pregunta también es muy relevante y se refiere a si se si el escaneo de material En búsqueda de abuso de material de abuso sexual infantil debería limitarse Por decirlo de alguna manera a Fuentes abiertas como foros redes sociales blogs etcétera o si a partir de ahora se debería monitorizar también el ámbito privado Como por ejemplo mis conversaciones entre yo y tú querido oyente porque ahí ya entramos en el ámbito privado pues eso es lo que pregunta está lo que se pregunta aquí no vale ahora que entendemos Cuáles son las preguntas que se han hecho todos los países qué ha contestado

España porque España ha sido la más radical y bajo mi punto de vista personal que no deja de ser más que una opinión de tantas esto ya sabéis que me gusta recalcarlo una cosa es la noticia y cuando yo doy una opinión personal puedo estar perfectamente equivocado o tener la idea equivocada o simplemente pues una postura que no compartís para mí ha sido España la postura más radical y para mal a la pregunta de si deberíamos debilitar de alguna forma el cifrado De extremo a extremo para que las empresas pudieran acceder a ese contenido ante una petición de gobierno España fue Clara y directa os Leo el principio de su respuesta Vale dice esto si se emite una orden de detección relacionada con el uso de material de abuso sexual infantil cifrado dicho material cifrado puede verse significativamente afectado en primer lugar en muchos casos el proveedor de servicio de internet podrá acceder a los datos cifrados esto significa que el proveedor puede tener la capacidad de descifrar el material de abuso sexual infantil cifrado en segundo y sé que es un poco rocambolesca la respuesta pero yo os la estoy leyendo como lo ha dicho España en segundo lugar La autoridad de la aplicación de la ley lea por sus siglas en inglés podrías solicitar acceso al material cifrado y si el proveedor de servicios de internet se niega a proporcionarlo la lea podría presentar una orden judicial para obtener acceso a los datos cifrados si se emite la orden judicial Entonces el material cifrado podría ser descifrado y aquí viene la clave aquí viene lo que hace de esta noticia una noticia el siguiente párrafo que ha dicho España textualmente idealmente desde nuestro punto de vista Sería deseable legislar para evitar que los proveedores de servicios con sede en la Unión Europea implementen el cifrado De extremo a extremo que os he querido decir con todo esto porque España básicamente quiere prohibir la implementación De cifrado extremo a extremo una capa de seguridad vital para nuestra privacidad de nuestras comunicaciones incluso ante las empresas que no están proveyendo el servicio esto a mí me parece bastante llamativo Y la verdad tendremos tiempo para debatirlo pero me parece bastante mal esta postura así tan radicales que estamos hablando de eliminar el cifrado extremo extremo dándoles la capacidad a todas las empresas que manejan nuestras comunicaciones de poder observarlas y si os fijáis en la propia respuesta de España habla de que si el gobierno lo pide al eliminar al cifrado extremo extremo las empresas van a poder dárselo y si se niegan a dárselo Entonces es cuando van con una orden judicial O sea ya plantean aquí el acceso a esa información sin ni siquiera una orden judicial Pero bueno continuo a la pregunta de si las empresas que así lo decidan deberían seguir pudiendo vigilar los datos de sus clientes En búsqueda de material relacionado con el abuso infantil España dice que sí que lo apoya es decir esto de que como os decía Apple y Google y Facebook Pues escanean un poco las fotos en búsqueda de material de pornografía infantil No pues España sigue apoyando eso a la tercera pregunta de si se debería incluir el audio en las búsquedas de material de abuso sexual a menores recordar que las empresas también puedan acceder a nuestro audio España dice lo siguiente Estamos de acuerdo en incluir las comunicaciones de audio en el ámbito de la propuesta del csa creemos que tal como lo propuso la delegación húngara la propuesta debería eliminar las referencias froncletas a los diferentes tipos de materiales imágenes textos vídeos o audios Y ser más general para abordar cualquier tipo de material relacionado con el abuso sexual en línea Es decir España aquí lo que está diciendo es que se debería de escribir la el reglamento de manera más genérica para que no se especifique individualmente Qué tipo de material sino que abarque cualquier cosa y así ya pues pueda decidir el gobierno un juez si entra dentro de la normativa O no normalmente para que os hagáis una idea queremos leyes Cuanto más específicas mejor bueno Supongo que dentro del caso pero cuando hablamos estamos hablando de temas de privacidad de espionaje y cosas así pues queremos cosas muy concretas aquí España dice no sólo que se debería incluir el audio sino que deberíamos eliminar totalmente el decir específicamente Qué tipo de material es y simplemente que abarque más cosas ya por último la pregunta de si la detección

debería solo limitarse a Fuentes abiertas sino también incluir las comunicaciones privadas me imagino que nos sorprenderá que España haya contestado lo siguiente como lo hacen los principales proveedores de servicios en Estados Unidos la detección automática de contenido las comunicaciones interpersonales es fundamental la detección automática Se informa al usuario los términos de uso de los servicios de manera que no se infrinja el derecho a la privacidad del usuario bueno Esto de que por mucho que te lo notifiquen pero si de repente es una normativa es que no tienes otra opción la opción es vale me desconecto totalmente de internet y de utilizar cualquier tipo de App y así claro que me digas que así no es infrija el derecho a la privacidad no se infringe porque básicamente me No si quiero utilizar algo pues no puedo esto es como algo que a mí personalmente me pone muy de mala leche no sé si a ti Alexis pero sobre todo aquí en España macho cada vez que llamo atención al cliente de algo a mi banco Así es esta conversación será grabada y alguna vez les he dicho Oye es que no quiero no quiero que se grabe y me dicen Ah pues entonces no te podemos atender o sea vale o sea entiendo esto es un poco como lo que dice España aquí no como lo que plantea vale vale No no protegemos tu privacidad si tú tienes derecho a negarte Pero entonces te niego el servicio pues tío eso no es darme una opción eso es decirme si lo usas es bajo mis condiciones que es violando tu privacidad y si no pues no lo puedes usar hombre las cosas no son así sí no en Estados Unidos también el tema es muchas veces si no todas esta grabación se se guardará para temas pero lo venden bastante bien lo venden para mejorar el servicio no en plan si no no te ofrezco servicios o sea son bastante listos Sí pero ya te digo yo aquí me he negado muchas veces en diferentes servicios primero se quedan un poco como hostias la primera persona que me lo dice Pero dice Ah es que si no no te puedo dar servicio si no me autorizas a grabarte y digo Siempre tú no me tienes que grabar para darme el servicio esto lo quieres hacer tú a mayores por la razón que sea pero aparte no te hablo de servicios que yo puedo Bueno pues tengo que ir a la oficina y ya está no no servicios de banca online que no tienen ni oficinas Entonces cómo me vas a prestar servicio o sea es que es como como una extorsión o me permites que te grabe o no te doy ningún servicio a mí me parece increíble eso pero la película de espía no en plan Perdona me puedes llamar por una línea segura que esta no no confío en esta línea escucho Pues bueno Ahí lo tenéis la postura de España es Clara han dicho a todo que sí monitoreo de conversaciones privadas autorización a las empresas a seguir escaneando a sus usuarios incluido el audio en la lista de los datos a escanear y lo más controvertido de todo y lo que realmente En mi opinión hace esto una noticia la prohibición del cifrado extremo extremo cágate lorito por contrapartida porque me he leído los los veintipico países sus respuestas y os dejo el documento por supuesto en las notas del episodio me gusta especialmente lo que ha contestado Alemania respecto al cifrado extremo extremo Y por cierto Italia también son dos de los países que se oponen a la eliminación del cifrado extremo extremo Alemania dice lo siguiente las disposiciones planificadas del reglamento de csa deben proteger los derechos fundamentales especialmente en lo que respecta a la confidencialidad y privacidad de las comunicaciones el Gobierno Federal es decir Alemania tiene serias preocupaciones acerca de las disposiciones sobre órdenes de detección en el reglamento propuesto para el Gobierno Federal es esencial garantizar un alto nivel de protección de datos y ciberseguridad incluyendo el uso de cifrado de extrema extremo completo y seguro en las comunicaciones electrónicas con esto en mente Alemania considera necesario entre otras cosas establecer en el texto del borrador que no se utiliza rán tecnologías que interrumpan debiliten eludan o modifiquen el cifrado pues ya tenemos un poco las dos posturas No qué opinas tú querido oyente a mí por un lado Me gustaría saber en qué se ha basado España para dar una opinión tan fuerte y directa hasta el punto de sugerir la prohibición del cifrado extremo extremo A quién han consultado para llegar a un consenso para que esa fuera la postura oficial de España Han opinado Solo

políticos como Javier zarzalejos del partido popular que ha sido el ponente de la Norma han incluido a mayores solamente a representantes de las fuerzas y cuerpos de seguridad o como en mi opinión Debería ser el caso se han juntado también con expertos en ciberseguridad y privacidad con opiniones a favor y en contra para llegar a un consenso la verdad es que es algo que a mí me encantaría saber muchas veces no sabéis dicho queridos oyentes que os encantaría que te iba de hackers empezar a hacer entrevistas a mayores del podcast yo Siempre os he dicho que no me gusta hacer algo que ya hacen otros podcast perfectamente porque es bueno es un poco repetir lo mismo pero sí estoy trabajando en una sección de entrevistas pero diferente y se me ocurre proponerle a este eurodiputado español una entrevista con tierra de hackers para debatir sobre su postura debatir porque España la postura oficial de mi país es que el cifrado extremo extremo debe de estar prohibido en Europa sería muy Guay yo le voy a contactar desearme suerte porque sería increíble si me dijese que sí y ella Alexis Te propongo una cosa porque ya sabemos que siempre queremos enseñar las dos caras de la moneda en tierra hackers Entonces te dejo elegir postura y debatamos un poquito yo encantado de Porque al fin y al cabo la no podemos olvidarnos de que aquí estamos hablando de detectar material de abuso sexual infantil Es decir de pillar a pedófilos y meterlos en la cárcel para que se pudran el resto de su vida Eso sobra decir que a todos es lo que deseamos la cuestión es los peligros cuando empezamos a legislar en base a una razón es totalmente loables y justificables pero que abrimos la puerta a situaciones y muy complicadas que vemos en países tampoco democráticos como china Al fin y al cabo aquí tenemos a China siempre criticando de que ellos no permiten el cifrado extremo extremo que todas empresas allí el gobierno tiene que tener acceso joder si nos deshacemos por ley del cifrado extremo a extremo nos estamos poniendo la altura de China que sí con la con la moralidad europea que se supone que es buena con las leyes europeas que son más potentes sin que Europa sea que bueno en este caso no es un país en Sí pero digamos que no tenemos una situación dictatorial Pero insisto estamos abriendo las puertas a que básicamente nos monitoricen sin orden judicial en base a la respuesta española nuestras Comunicaciones y esto Empezando por las empresas privadas que son las que procesan nuestros datos entonces Alexis debatamos un poco quieres pillar tú la postura defensora del cifrado extremo extremo o la postura española de deberíamos deshacernos de ello y debatamos un poquillo la verdad sinceramente yo sin ser un experto y a vote pronto A ver déjame pensar estaba pensando algunas ideas Pero bueno ya que me ya que me haces la pregunta de forma tan seria podría decir que se me ocurren tres medidas para mantener el cifrado extremo a extremo y evitar el abuso de menores el primero podría ser si la policía tiene sospechas de algún usuario pues pedir una orden judicial para que le den el permiso de poder comprometer hacer hackear digamos explotar los dispositivos de estos sospechosos y de esta forma poder acceder a los datos cifrados extremo a extremo y esto lo hemos visto más de una vez como gobiernos utilizan pegasus y otros spywares similar para acceder a datos no porque estén cifrados extrema extremo en muchos casos sí sino porque quieren tener datos en tiempo real y rastrear a esas personas y bueno Más allá de lo que es acceder a datos cifrados extremo no pero esa sería la primera la segunda sería pues no aplicar cifrado extremo a extremo a los menores porque pensándolo un poco en específico en el tema del que hablamos No del crimen de abuso de menores normalmente el criminal cultiva una relación online con la víctima menor de edad durante un tiempo Pues si de nuevo si sospecha de algún usuario que está intentando crear esta relación de proximidad no de afecto con un menor de edad pues Oye si el menor de edad no tienes tiene sus dispositivos y no los tiene cifrados extremo a extremo pues es mucho más fácil acceder a los datos del menor con la idea de pillar Al criminal y la última Pues como siempre creo que siempre hay un factor en todo el tema de la ciberseguridad que es la educación la concienciación no que es lo que intentamos

hacer desde aquí desde el podcast para todos nuestros oyentes No pues en este caso sería que en las escuelas se hablara de este tema se educar a los menores sobre todo este tipo de abuso infantil abuso de menores y sobre todo como digo el tema de de esto que se hace cultivar relaciones online en chats en sitios que en los que a veces los menores pasan mucho tiempo no como juegos online el vídeo en videoconsolas y en los chats relacionados con estos juegos en los que a veces incluso ellos no se dan cuenta que están hablando con alguien que podría ser una amenaza para ellos y los padres tampoco se dan cuenta de este riesgo de que no mi hijo está chateando en un videojuego con alguien pero probablemente sea un amigo no o alguien como él de su edad que está jugando pero no pueden hacer pueden ser ahí pues esas esas personas con Malas intenciones no con Los menores O sea tú lo que propones si te he entendido bien es por un lado el derecho a hackear a los malos utilizar exploits de cero de ellos o sea que los gobiernos puedan empezar a utilizar los pegasos y tal contra los malos algo que realmente se está haciendo pero no de manera pública esto no salen los presupuestos esto no sale la prensa cuando hace declaraciones sabes los esfuerzos y cuerpos de seguridad no te dicen Ah pues mira justo hemos comprado este exploit y se lo hemos lanzado y tal y cual no vale tú propones eso y luego por otro lado que eso es decir que me parece interesante es que se digamos que se puede interceptar las comunicaciones solo de menores bueno eso técnicamente Sería posible porque tú cuando te registras en un servicio tienes que poner tu edad entonces se podría detectar ahí incluso a lo mejor pues yo que sé se podría hacer un rollo aunque ya sería más difícil de consentimiento explícito de los de los padres de que se pueda monitorizar sus comunicaciones no Y si se detecta algo pues que salte claro yo ahí veo un problema el problema que por ejemplo era lo que planteaba Apple contra el FBI no que es en el momento que tú desarrollas tecnología para saltarte un mecanismo de seguridad es que lo van a encontrar también los malos entonces para hacer eso para menores claro a ver podrías a unos ponerle cifrado extremo extremo y otro no no se trata de poner una puerta trasera en el cifrado extremo extremo que aplique solo con menores Pero bueno Luego también Es verdad que los chavales tienen los mismos derechos que los adultos también no a su privacidad Entonces eso también puede ser un peligro Y luego quién te dice que sea lo que pasa que me acabo de dar cuenta que ahora estoy he vuelto yo al lado de defender yo de estaría debería estar diciéndote que sí claro bueno ha sido un debate un poco raro no porque yo se supone que estoy del lado de España y te estoy diciendo no no hay que hacer eso y más y más bueno que me parece me parece un planteamiento Interesante pero difícil de implementar la verdad que fuese Solo que se interceptase solo para para Al fin y al cabo algo que quería comentar creo que hemos criticado mucho a por ejemplo a tiktok no pero según Tengo entendido últimamente están poniendo las pilas mucho en verificar si una cuenta pertenece a un menor o no así que es algo que porque a ver tú puedes ir ahí a crearte una cuenta y decirle el año que te dé la gana no en plan aunque tenga 14 pongo que tengo 20 años o 30 o los que quiera pero no lo tengo muy claro cómo lo hacen Pero de alguna forma creo que o requieren verificación o luego lo que hacen También es miran los vídeos que ponen claro esto ya es no es extrema pero son vídeos Pero bueno Supongo que un tema es son los vídeos que exponen públicamente otro tema sería comunicaciones que van a través de la mensajería de esa plataforma social que podría ir extremo a extremo Entonces si ven que la mayoría de los vídeos tienen una cara que se corresponde con la de un menor Oye pues a estos a esta mensajería no lo voy a aplicar el extremo extremo por ejemplo de como idea vale el tema ahora volviendo yo pillando la postura española tu mecanismo realmente no serviría de mucho porque solo servirían la parte de tú estás grabando o haciéndole grooming a un menor pero muchísimos casos que sucede te lo digo porque yo estuve hace un mes con Naciones Unidas en Filipinas pues trabajando con fuerzas y cuerpos de seguridad allí para pues para darles clases sobre Cómo investigar y

encontrar a gente que se dedica a a enviar y a Bueno pues a intercambiar este tipo de material realmente el problema cuando lo tenemos que detectar es en el intercambio entre adultos porque muchas veces esto sucede en que se va el malhechor a países como filipinas abusa allí graba material allí en directo y lo distribuye entre adultos por tanto el mecanismo que en ningún momento hay una comunicación porque esto pasa sobre todo mucho en países pues subdesarrollados no donde pues las familias pasan muchos apuros económicos Entonces no serviría tu medida necesitamos deshacernos del cifrado extremo extremo Porque necesitamos poder monitorizar las comunicaciones entre adultos que se intercambian este tipo de material Sí también a mí yo me estaba yendo más Al Punto Final donde al final Al fin y al cabo tiene que haber un menor ahí Pero obviamente cuanto antes Claro pero no tiene por qué ese menor ese menor no tiene que haberse comunicado vía digital con su agresor por eso te hablo específicamente de países como filipinas Sí pero no sé asumiendo que hoy en día Todo va vía internet incluso las comunicaciones de voz que estabas comentando el tema de deberíamos incluir el audio o no entonces ahí también hay otro tema que se podría barajar Pero entonces dejamos desprotegidos a los menores que son capturados o simplemente se les paga para para engañarles y que llevan a casa a cabo este tipo de actos con eso lo he pincelado brevemente antes pero me refería un poco a educar a estos menores también porque no todo es digamos datos y privacidad Pero educarlos y entrenarlos en estos temas específicos y también ponerles rastreadores por ejemplo como airtags y similares para saber dónde están si se está moviendo Bueno pero esos son Sí pero eso digamos que de aquí a que en todos los países insisto la mayoría de estos problemas suceden países subdesarrollados ahí no tienen temas de bueno no quiere decir que no tengan temas de alerta pero tú me entiendes lo que quieres decir tecnológicamente no están tan desarrollados la educación muchos casos lamentablemente es hasta consentido es más prostitución infantil que el que vayan Y rasten a niños para obligarles a hacer esto Hay a veces que es consentido por el menor que bueno con sentido entre comillas porque un menor realmente no no sabe lo que está consintiendo no en cierto sentido Entonces sí que das medidas que podrían solucionar ciertos casos pero yo como España sigo insistiendo poniéndome en el papel de España aquí figurativamente para hacer el papel del debate no estamos protegiendo a todos los niños por tanto exijo que nos deshagamos del cifrado extremo extremo qué me dices No lo sé de nuevo no soy experto en el tema y me pillas a bote pronto pero no sé igual se podría intentar a ver yo no creo que sea tanto el ahora mismo que encuentres una solución efectivamente como bien explicas tú a un problema tan complejo es como si te digo ahora Oye solucióname el viaje en el tiempo cómo lo hacemos No esto hay que darle una reflexión me refería yo iría más ahora volviéndome a la parte donde yo estoy en la postura en las implicaciones de hacer esto Esto es un poco como lo podemos poner de otra manera permitiríamos que el gobierno entrase en nuestras casas sin ningún tipo de orden judicial cuando ellos quisieran Si eso en principio según ellos lo hacen para proteger a los menores de abuso sexual claro ahí ahora ya es como más visual no en los tras de repente a las 3 de la mañana puede entrar aquí un agente a revisarme todos los cajones no a ver que en realidad normalmente Pues hay indicios y todo esto no Pero a lo mejor así el público entiende un poquito mejor no todos todos decimos no no en mi casa no entra nadie sin un sin una orden judicial claro eso es un tema Se podría poner algo así como tú dices en lugar de tener cogiendo la analogía de la casa en lugar de tener una cámara grabando constantemente 24 por 7 podría ser una cámara que está apagada y el dueño del gestor de esa casa no los inquilinos la enciende a petición de los policías que quieren investigar algo y les dejan saber a los inquilinos que Oye voy a encender esta cámara ahora o la cámara está encendida hay un poquito al menos Aunque pueden ver tus datos pero no los están viendo todo el rato y si quieren apropiarse de más datos que no sean los actuales Pues no sé debería alertarte también o pedir

una orden judicial de nuevo vuelvo al mismo tema de que quede algún tipo de registro y que se haga la gente digamos responsable de lo que de lo que bien venga después claro aquí e insisto eh que yo mi postura es que el cifrado extremo extremo debería permanecer ni de coña ni de coña deberíamos eliminarlo o prohibirlo que es lo que está diciendo España Pero sí he de decir que que a día de hoy con orden judicial tú puedes interceptar comunicaciones las llamadas telefónicas de toda la vida en España con sitel creo que se llama tú puedes acceder a un hogar con una orden judicial Entonces si la propuesta fuera Oye con orden judicial deberíamos poder acceder a tus comunicaciones por WhatsApp o Signal entonces en principio ahí por un lado no cambiaría tanto el escenario Porque si día de hoy estamos Ok con que con una orden judicial tú puedas entrar un hogar con una orden judicial tú puedas interceptar llamadas telefónicas Por qué No deberíamos estar de acuerdo que con una orden judicial tú puedas interceptar llamadas telefónicas por void o mensajes o mensajería a través de Signal Telegram O WhatsApp claro no cambiaría mucho Yo creo que un problema fundamental es la implementación que eso es muy complicado porque tú ahora estás reduciendo Estás debilitando una protección que que en parte salen la Carta Magna artículo 7 como decía que es el derecho a la libertad de expresión es el derecho a poder comunicarte de manera privada entonces claro No yo creo que requiere como mínimo de más debate por eso preguntaba que no sé cómo España ha llegado al consenso de que esa es la postura oficial del país el Oye vamos a pedir que se elimine esto que garantiza unos derechos fundamentales de los ciudadanos sobre todo en Europa que que velamos bastante por la privacidad no nos han consultado Martín cuando hicieron el Draft el borrador de esta propuesta ley de quitar el cifrado extremo extremo no el falto de invierno por eso por eso quiero Por eso quiero invitar a este eurodiputado a un debate para que bueno Pues a lo mejor nos dé una visión más clara de su postura y a lo mejor pues convence a toda la audiencia desde luego la audiencia de tierra de hackers que estamos en los miles y miles y miles es perfecta para convencer no Oye si de verdad Viene con una argumentación sólida Oye Aquí no se trata de venir a no no esta es mi postura ya está yo estoy más abierto a estar equivocado a cambiar de postura yo no vengo aquí con una radicalización tengo unas convicciones creo que con fundamento basadas en unas yo creo insisto argumentaciones sólidas Pero por supuesto estoy dispuesto a debatir con quien sea y que me haga cambiar de opinión Pero bueno pues no alargar esto más que llevamos un rato Espero que os parezca el último comentario Yéndome a un extremo más allá en tu en tu parte en tu punto de vista no que defiendes el tema de eliminar el cifrado extremo extremo sería Oye si no Espera espera vamos a matizar eso vamos yo no defiendo estaba haciendo el papel de España en este debate pero pero mi postura es que no deberíamos eliminar comunicaciones seguras que permiten la comunicación privada sin sin estar ante los ojos del gobierno Este era un role play como se dice no pues el ro Martín estaba estaba utilizando quería ir un poco más allá también en plan la típica pregunta esa no que igual el este eurodiputado te haría hombre si tú no tienes nada que esconder por qué quieres por qué necesitas el cifrado extremo extremo y le puedes decir Bueno es muy claro porque no has visto todas las brechas de seguridad si si me viene aquí Cualquier gobierno o cualquier empresa privada que trabaje para un gobierno que son normalmente las que hacen el trabajo sucio porque el Gobierno no tiene no quiere mojarse o no tiene suficientes empleados para hacer esto mira incluso empresas de seguridad las las comprometen y los datos que tienen de cualquiera de sus objetivos salen al público se venden en la Dark web y ahora quieres que además de que puedan comprometer la plataforma que tiene mis datos que podría ser Google o Apple también mis datos están expuestos ahora en otra plataforma que es la de este esta empresa privada que está intentando evitar el abuso sexual debería de haber alguna forma mejor Mira yo le contestaría directamente con la famosa frase que de hecho en la conferencia

de sintomáticos tenía una diapositiva con esa con esa esa famosa frase atribuida Edward snowden que dice algo así no me la sé de memoria pero viene a decir que no te importa el derecho a tu privacidad porque no tienes nada que esconder es equivalente a decir que no te importa el derecho a la libertad de la ex de expresión porque no tienes nada que decir o sea el hecho de que yo no tenga nada que ocultar no quiere decir que no sea importante el tener una privacidad una intimidad sabes no solo los delincuentes debería preocuparles la privacidad es que eso es básicamente lo que estaríamos diciendo la gente que dice yo no tengo nada que ocultar entonces me da igual que me miren todo Ah entonces solo a los de estamos diciendo que solo los delincuentes les importa la privacidad eso es completamente absurdo y también siempre algo que esconder mentiras piadosas en plan estoy preparando una fiesta de cumpleaños o de aniversario a mi familia algún familiar mío y te sale ahí bueno hombre pero es al gobierno es el gobierno le da igual Pero oye imagínate se me ocurre así a vote pronto algo que no es ilegal pero que quieres ocultar por ejemplo hace 20 años donde estábamos con los derechos del colectivo lgtb no es donde estamos a día de hoy y te aseguro que hace 20 años había tanta gente de ese colectivo como la hay Ahora solo que hace 20 años era mucho más peligroso para ellos que eso se supiera Entonces ese es un claro ejemplo de lo necesario que es la privacidad y la intimidad tú Imagínate que vives en un gobierno de hace 20 años cuando ser homosexual o del colectivo lgtb podía ser un problema hasta para tu seguridad física Entonces por supuesto que es importantísimo tener internet más claro tu preferencia política ya sin tener en cuenta el tema es eso es política importante no Yo quiero poder tener las conversaciones con mi cuñado de política por WhatsApp pero no no efectivamente no hace falta delinquir para para que la privacidad sea útil o tenga valor para nada en fin os dejo con la pregunta del episodio queridos oyentes nos vamos al comité de sabios que sois vosotros estás A favor o en contra de la postura de España de que se debería prohibir el cifrado extremo extremo os doy dos opciones a favor de que se prohíba en contra de que se prohíban ya sabéis contestarnos en Twitter arroba tierra de hackers debate calentito Y si queréis poner algún motivo pues mucho mejor y alguna también nos podéis preguntar para cuando venga el señor eurodiputado No pues nada Es que os dejo un tweet de él porque me fui a su Twitter lo busqué para que o sea se me fue el santo al cielo quería decir que busque su Twitter para ver si hacía referencias a esto y efectivamente tiene tres tweets enlazados donde habla de esto y comenta que lo necesario que es y su postura entonces yo le voy a mencionar en Twitter a ver si cuela y se apunta a venir a hablar con nosotros por qué no sería muy interesante Pues nada espero vuestras respuestas y nada muy interesante Martín mucho mucho que pensar Pero nada vamos con la siguiente noticia que va de canales laterales que hemos comentado anteriormente es decir cómo se pueden robar datos de un usuario es decir tus datos querido oyente online de una forma indirecta Incluso si el cifrado de extremo extremo está activado por ejemplo Y es que un equipo de académicos de las universidades norteamericanas Georgia Tech y Michigan y La alemana de hecho estas universidades siempre traen buenos informes y hemos cubierto varios de ellos de estas universidades Pues un conjunto de académicos de estas tres universidades ha publicado un informe que detalla múltiples ataques de canal lateral que afecta a procesadores Arm y gpus a procesadores que se centran en la renderización de gráficos los procesadores Arm son muy populares probablemente los conozcáis os suena y se encuentran en el corazón de dispositivos de Apple como iphones y macbooks y otros teléfonos Android como los Google Pixel y One Plus 10 pro y comento estos tan específicos porque son los que se probaron en este estudio el ataque en concreto se basa en utilizar los sensores internos físicos para medir los cambios de frecuencia potencia y temperatura y poder inferir y robar los datos procesados por el sistema que de otra forma sería imposible obtener en un ejemplo el equipo de investigación dice que usaron código javascript para robar historiales de

navegación y píxeles mostrados en la pantalla es decir una imagen de navegadores como Chrome y Safari incluso cuando los dispositivos tenían habilitadas todas las contramedidas de canal lateral conocidas esta investigación es la última de una larga lista de ataques de canal lateral que tienen como objetivo el escalado Dinámico de voltaje y frecuencia o del inglés voltage frequency skyling que es una función de ahorro de energía utilizada por chips modernos es decir que el procesador va más rápido consume más energía y se pone más caliente cuando tiene que procesar más instrucciones y más datos por ejemplo como cuando te pones a crackear los hashes de contraseñas como parte de un trabajo de seguridad Legítimo para explicar esta funcionalidad escalado Dinámico de voltaje y frecuencia os voy a dar el ejemplo o analogía de un coche que va por la carretera digamos que a una velocidad específica el motor va a una frecuencia F consume una cantidad de energía e y está a una temperatura t si el vehículo va más rápido obviamente las variables feit van a incrementar y el caso sería el contrario sí disminuye de velocidad Pero hay casos interesantes como encender el aire acondicionado o subir o bajar las ventanillas que requiere de energía adicional lo que puede incrementar ligeramente la frecuencia del motor y la temperatura del vehículo entonces midiendo y perfilando cada una de estas tres variables un ataque un atacante podría saber qué estás haciendo realmente en el coche si está subiendo la ventanilla o si estás si has encendido el aire acondicionado o temas similares o sea para que veáis un poquito como que con estas tres variables se puede jugar para realmente saber que se está haciendo dentro del coche en estudios anteriores se encontró que los chips Intel y amd también eran vulnerables a este tipo de ataque Los investigadores demostraron que los atacantes pueden utilizar javascript Como he mencionado anteriormente para manipular los píxeles de tu pantalla y medir el tiempo que tarda tu navegador Chrome Safari en renderizar ciertos elementos esta información puede utilizarse para determinar qué páginas estás visitando Incluso si estás utilizando una conexión segura Pero eso no es todo los investigadores también descubrieron que los atacantes pueden utilizar Esta técnica para robar datos confidenciales como por ejemplo Las Cookies de sesión lo que les permitiría hacerse pasar por ti en sistemas En plataformas online esto podría utilizarse Consecuentemente para realizar todo tipo de actividades maliciosas desde el robo de identidad hasta el fraude Financiero los ataques presentan los autores presentan varios ataques potenciales y son tres de hecho los que los que muestran uno es el robo de píxeles o la identificación de imágenes en el navegador web los ataques de espionaje del historial de navegación es decir que páginas has visto anteriormente Y la identificación de huellas digitales de sitios web otra forma de identificar Qué sitios web estás visitando los ataques de robo de píxeles pueden exponer información privada contenida en la imagen renderizada de una página web es decir por ejemplo si estás viendo una imagen de no sé de algo que te han enviado que tiene datos confidenciales Como pudiera ser una tarjeta de crédito o algún documento legal pues esto la imagen en Sí podría filtrarse a través de este tipo de ataques y como digo en este caso se basan en estos ataques se basan en medir las propiedades físicas de los dispositivos como el consumo de energía y temperatura y la frecuencia también del procesador y utilizar esta información para inferir los datos procesados por el dispositivo para poner una analogía para este caso específico del robo de píxeles podríamos pensar en que estás pintando un dibujo con diferentes lápices de colores digámoslo así Cada vez que cambias de color tienes que ir a limpiar tu lápiz en un papel tienes un amigo que está sentado a tu lado que no puede ver tu dibujo pero que puede ver el papel donde limpias tu lápiz al observar los colores que dejas en el papel puede adivinar qué estás dibujando a alto nivel en este caso tú eres el ordenador El dibujo es la página web los lápices de colores son los datos que procesas Y tu amigo es el atacante este ataque se lleva a cabo en concreto utilizando javascript en navegadores como Chrome y Safari y comienza con una fase de calibración donde se aplica y se

mide el tiempo de renderización de filtros de imágenes específico en ciertos píxeles conocidos para establecer un umbral un umbral de tiempo de referencia es decir primero se cargan unas imágenes es como un modelo de entrenamiento y cargas una imagen por ejemplo digamos de un pingüino y dices pues esta imagen del Pingüino se tardan 5 segundos ahora cargo una imagen de un león y esta imagen tarda 10 segundos pues se hace como una categorización una base de datos se definen estos parámetros para luego poder compararlos identificar imágenes que no tengas en perfiladas anteriormente después de hacer este esta fase de entrenamiento se inicia la fase del robo la fase del digamos la exfiltración de datos no donde se aplica y se mide el tiempo de renderización de filtros en un píxel objetivo de un elemento iframe cuyo contenido se puede acceder para el robo de píxeles esto lo que hacen es obviamente necesitas la víctima tiene que acceder a una página maliciosa pero lo que hacen es al visitar una página maliciosa controlada por el usuario y por el atacante cargan iframes que contienen páginas objetivo que quieren determinar quieren extraer información relacionada con tu con tu usuario online en esas plataformas Bueno lo que hacen luego es elegir un píxel de la página objetivo y utilizar ciertas funcionalidades de navegador web como css para convertir el valor del Pixel en negro o blanco y de esta forma maximizar el contraste y la diferencia y luego se aplican múltiples filtres filtros para determinar la diferencia con con los modelos de base y finalmente se clasifica el color digamos de Pixel en base al umbral de tiempo obtenido durante la calibración de esta forma se va Pixel por Pixel y se determina la diferencia de tiempo en base al modelo de referencia y así identifican el color de cada uno de los píxeles en la pantalla y a través de cada uno de los píxeles pues pueden reconstruir la imagen que se está mostrando en el navegador en Sí oye volviendo a lo del tema de detectar imágenes que hay que deshacerse De cifrado extremo a lo mejor así se podría hacer detecta imágenes de temas de pedofilia haciendo escaneo la digo a plan exagerado evidentemente esto es académico Pero mira ya no tendríamos que deshacernos de cifrado extremo extremo sí claro lo único que bueno si en este caso Igualmente están están violando tu privacidad No porque no les estás consintiendo pero a ver si si Sí sí pero por lo menos no se deshacen del cifrado lo estoy intentando OK Para que preservemos el cifrado extremo extremo sí pues el otro ataque es digamos de espionaje del historial de navegador web Pues de nuevo utilizando temas físicos midiendo frecuencia energía y calor del dispositivo el procesador pues Pueden saber las páginas web que has visitado anteriormente hace tiempo este ataque se podía llevar a cabo a través del Análisis del css mostrado al usuario en el navegador web a través de la identificación de si una URL específica digamos tierra de hackers.com es se ha visitado antes o no esto lo habréis visto porque en el navegador cuando vuelves a una página que tiene enlaces si los has visitado antes normalmente salen en color Lila y si no los has visitado salen en color azul Esto se está esta diferenciación se utilizaba antes cuando los navegadores web no implementaban medidas de seguridad contra este ataque para identificar las páginas web que habías visitado pero los navegadores modernos no permiten a día de hoy que javascript pueda determinar el valor de visitado o no en los links mostrados en la página Pues con Esta técnica se salta esta contramedida aún así y puede terminar qué páginas has visitado o y cuáles no y lo mismo pasa con temas de huellas digitales de sitios web lo que intentan hacer es identificar sitios web específicos a partir de sus patrones de asignación de memoria contención con otras cargas de trabajo de la de la cpu y la gpu consumo de energía y temas relacionados es decir en base al impacto que tiene en el sistema una página web que tienes actualmente cargada también puedes saber la página que estás visitando actualmente estos ataques son particularmente preocupantes Porque pueden ser llevados a cabo sin privilegios elevados y pueden ser efectivos incluso cuando se han habilitado todas las contramedidas de canal lateral además estos ataques pueden ser lanzados contra muchos dispositivos ya que los procesadores

afectados Arm y las gpu son utilizados en muchos dispositivos a nivel mundial esto como digo ataques de canal lateral No son nuevos y de hecho hemos cubierto algunos en episodios anteriores incluso ya desde los 90 han habido ataques similares de medición de parámetros físicos como ataques de temporización no que se basan en medir el tiempo que tarda un sistema en realizar ciertas operaciones para revelar información sobre los datos que está procesando hay ejemplos en los que se pueden extraer claves de cifrado por ejemplo rsa de sistemas en función del tiempo que tarda en realizar operaciones una un procesador una cpu también hay ataques de consumos de energía y también incluso ataques acústicos bueno y más No pero para que tengáis un ejemplo que esto no es no es nuevo ya desde los 90 pero están nueva forma es es novedosa básicamente aplicando el tema de frecuencia energía y calor al mismo tiempo para ex filtrar datos de procesadores los ataques descritos en la investigación afectan como digo procesadores Arm y gpus que están en muchos dispositivos pero los autores de este análisis utilizaron o probaron el ataque contra portátiles macbook Air M1 y m2 contra teléfonos inteligentes Google Pixel 6 pro y One Plus 10 pro y también contra tarjetas gráficas o las llamadas gpu nvidia geforce rtx 3060 y amd radeon RX 6.600 por poner un ejemplo de uno de los ataques el de recuperación de píxeles que es como el más hollywoodiense diría yo me lo imagino porque se podría hacer un ejemplo no hay vídeo no pero me imagino ahí el típico no que Martín que alguien va a una puerta y tiene una pantallita de introduce código van a ir siempre conectan no su móvil ahí que llevan siempre y lo dejan ahí y en el móvil van saliendo los numeritos dando vueltas del 0 al 9 y se queda un número fijo y va al siguiente dando vueltas de 0 a 9 Pues aquí me imagino igual te sale la pantalla toda en blanco y poquito a poco van saliendo los píxeles uno por uno Tic Tac del color que sea y se va formando un puzzle me recuerda un poco a las pantallas de carga de videojuegos de los ordenadores de los 80 y 90 ahí que va saliendo la imagen línea por línea correcto o bueno o también cuando cuando empezó internet lento a 33 600 baudios también las imágenes cargaban Pues imagínate en esto A ver dime por ejemplo en el en el peor de los casos no no en el mejor de los casos Cuánto tiempo necesita este ataque para recuperar un píxel a ver si puedes adivinar en el mejor de los casos claro no llegaste a decir si era algo viable o no pero quiero pensar si es Pixel Y tenemos imágenes de 1080 espero que sea una décima de segundo 8 segundos por Pixel ostra pues ya puedes tener paciencia Por ejemplo estaba haciendo un cálculo la verdad que es bastante por ejemplo pensando en nuestra imagen del episodio de tierra de hackers que son la corta 675 por 675 si multiplicamos por 8 segundos esto sale a unas Mil horas Claro que serían unos estoy haciendo el cálculo aquí realtime serían unos 42 días para intentar sacar toda la imagen Es que para eso casi Bruce la contraseña que sea y ya tienes acceso a todo a ver Esto me lo puedo imaginar estaría Guay para qrs no de Second factor autentication yo creo que ahí pues esa es una imagen que por encima los píxeles están súper marcados A lo mejor podrías hasta ignorar los blancos no sé pero bueno aún así es inviable o sea académicamente OK Pero no veo yo un ataque via por eso por eso ahora por ejemplo alguien puede hacer clic en plan o por qué tengo que si tengo si estoy solo delante de mi pantalla no y no hay nadie que me esté viendo la pantalla porque tengo que que proteger siempre mi contraseña y que salgan los asteriscos No pues ahora sabes por qué Porque si se estuvieran viendo los dígitos de tu contraseña que estás escribiendo un ataque como este lo podría sacar Aunque tardaría bastante tiempo pero igual si se enfoca en en un en un trozo de la pantalla que tiene muchos menos píxeles pues no sé pues igual los sacaría antes o incluso igual se podría optimizar no con temas de yo que sé Machine learning o el tema similares en plan voy a de cada 10 píxeles solo necesito tres para determinar con 90% de precisión si es un cero o un uno o algo así anyway eso se tardan 8,1 segundos en recuperar un píxel en una gpu amd radeon RX 6.600 con una precisión del 94% pero en el en el peor de los casos en el en el otro extremo tenemos que una gpu Intel Iris XE se tardaron 22,6

segundos en identificar cada uno de los píxeles con una predicción del 77% y luego tenemos entre medio diferentes valores de para otro dispositivo no la nvidia geforce rtx 3060 para esta se tardan 8,7 segundos por Pixel para el Google Pixel valga la redundancia 6 Pro se tardan 9,6 segundos por Pixel oneplus 10 Pro se tardan 18,9 segundos por Pixel aquí ya empieza a incrementarse bastante el tiempo por Pixel los macbooks se tardan unos 20 y 22 segundos por Pixel Así que se podría decir que si utilizas un macbook Air M1 m2 no es que estés protegido porque Igualmente se puede llevar a cabo este ataque pero es sería en el caso que se tardaría bastante en recuperar lo que esté mostrando por pantalla los autores comentan que es importante destacar que esos ataques no se limitan a estos dispositivos específicos que han probado como digo macbook pros amd radeon RX y nvidia geforce y teléfonos móviles sino que cualquier dispositivo que utilice un procesador Arm o una gpu en plan genérica y que permite la ejecución de javascript en un navegador podría ser potencialmente vulnerable comentan algunas limitaciones y es que estos ataques se centran en dispositivos que ellos comentan que son térmicamente limitados vamos que no pueden superar una temperatura específica entonces Claro si estos ataques se basan en medir diferencias de temperatura y llega a un nivel específico donde ya no puede subir más pues obviamente están limitados de alguna forma también las variaciones en la frecuencia y el consumo de energía son muy pequeñas en procesadores y gpus modernas lo que requiere periodos de muestreo más largos para observar diferencias de tiempo significantes o sea como hemos dicho es un es un ataque muy muy académico con muy poca probabilidad de ser aplicado en la vida real Pero bueno igual lo mismo pensábamos de romper temas de cifrado no pero cuando llegue la computación cuántica pues Oye veríamos el pasado como algo posible en el presente las mitigaciones propuestas incluyen temas tanto de Hardware como de software en el lado Hardware los autores sugieren el uso de refrigeración activa para los dispositivos técnicamente limitados y la operación del sistema por debajo de los de unos niveles específicos de energía o de temperatura de esta forma cuando lleguen a ese cierto límite pues no no van a variar esas dos variables y solo van a tener una variable como digo este ataque un poquito se basa en tema de lo podemos ver como una triangulación no en el campo de del espacio en la geolocalización tú puedes identificar a un individuo con tres puntos puedes saber dónde está si tienes dos es bastante menos preciso y si tienes uno es bastante muy poco preciso No pues claro el tema de que cogen Tres puntos de apoyo en este ataque como digo frecuencia energía y temperatura pues les ayuda mucho más para identificar realmente los datos que están procesando Así que una de las mitigaciones es a nivel de Hardware intentar limitar una o dos o todas de estas tres variables en las que se basa el ataque en el lado del Software se sugiere aislar por ejemplo Las Cookies de los iframes de origen cruzado Es decir de una de un sitio web al otro no entran en estos detalles pero básicamente que no se puedan acceder a las cookies entre distintas páginas web distintos iframes cuando tienen un origen distinto es decir una URL distinta y prohibir que los filtros de imágenes svg que son los que se han utilizado en este ataque se apliquen a iframes o hipervínculos Esto bueno requiere bastante modificación del navegador web no sólo eso sino también digamos del diseño y la definición de los protocolos html y similares además los ataques de huellas digitales de sitios web pueden mitigarse si los proveedores de sistemas operativos eliminan el acceso no privilegiado a las lecturas de sensores que es otro punto también interesante porque una aplicación un poco el modelo igual de seguridad que tienen los teléfonos móviles no en plan si tienes una aplicación instalada en tu sistema de escritorio o laptop igual debería implementarse algún modelo de seguridad que exponga ciertos componentes del sistema y que esta aplicación los pida o que el usuario los autorice en plan esta aplicación está pidiendo acceso a sensores físicos de temperatura y tú vas y dices pero si es la aplicación si es el mi gestor de correo porque necesita acceso a esto Entonces algo

sospechoso No pues igual algo así se podría implementar que ya se hace por ejemplo un poquito como digo en móviles iPhone Android Aunque iPhone bueno viene viene dado un poco por el tema el modelo de seguridad de Apple pero en navegadores web por ejemplo las extensiones también te dicen a que componentes A qué datos del navegador pueden acceder o quieren acceder o no así que sería otra forma de delimitar el tema El documento concluye que la frecuencia de regulación es parte de un equilibrio entre la velocidad de ejecución el consumo de energía y la disipación de calor los autores demuestran que los ataques de canal lateral son posibles en gpus y procesadores Arm Especialmente cuando uno de estos factores se limita es decir que aunque se limite uno de ellos todavía se tienen datos suficientes para con menor precisión y llevar a cabo el ataque autores concluyen que es importante ser consciente de estas posibles amenazas y tomar medidas para protegerse Aunque estos ataques pueden ser difíciles de llevar a cabo pero aún así representan una amenaza potencial y es importante tomar medidas para mitigar estos riesgos como digo a nivel de usuario nosotros no podemos hacer mucho al respecto es más tema de fabricante de dispositivos a nivel Hardware las medidas que he mencionado y a nivel de software pues tema de navegador web a no ser que hay alguna extensión por ejemplo que permita por ejemplo lo que he mencionado no que prohíba el uso de filtros svg en iframes o hipervínculos igual se puede crear algún tipo de extensión para navegadores web para implementar esto pero bueno como hemos mencionado antes el tema de ex filtrar una imagen tarda bastante tiempo así que no es algo que sea preocupante a día de hoy pero es algo a lo que de lo que se tiene que ser consciente y cerrando ya la noticia lo que es realmente fascinante sobre estos ataques es que muestran que cuán profundamente se puede llegar a la información Incluso en sistemas que parecen seguros en la superficie no por ejemplo estamos hablando del tema de aunque aunque tuviera en tu encription si se está mostrando la imagen que tiene cifrada extremo a extremo en el navegador web con este tipo de ataque se podía se podría capturar y ex filtrar y lo que es aún más sorprendente es como estos ataques pueden aprovechar características que son fundamentales para el funcionamiento de nuestros dispositivos y sobre todo son temas físicos es aquí de nuevo como el tema digital o Cibernético se mueve al tema físico Para volver de nuevo y determinar temas digitales de tus datos es como bastante interesante este ciclo este Loop retroalimentado no y es que está la frecuencia de regulación dinámica de voltaje es una característica esencial que ayuda a nuestros dispositivos a equilibrar el rendimiento y el consumo de energía y Por ende a que nuestro dispositivo pues sean más rápidos se corran mejor no y que duren también más pero en manos equivocadas Como pudiera ser un cibercriminal podrían convertirse en una herramienta para espiarnos y robar nuestra información privada pues tal cual lo que dices Alexis es a eso que me refería que las fuerzas y cuerpos de seguridad en vez de deshacerse del cifrado extrema extremo puedo utilizar técnicas como esta para ir a por el sospechoso específico intentar averiguar así si tiene imágenes de pornografía infantil así ya no nos tenemos que deshacer de Bueno claro si te deshaces de El problema es que tener que utilizar este tipo de exploit o cosas así es algo activo no tienes que tú no puedes hacerlo a escala tienes que seleccionar a tu objetivo y luego hacer todo esto en el momento que no la medida de deshacerse del cifrado extremo extremo es algo pasivo le quitamos la seguridad a todos y ya luego dejarnos a nosotros ir a mirar solo los que deberíamos entonces claro yo prefiero un poco la parte activa no no que tengamos todos una buena seguridad y ya tú empleas tus metodologías avanzadas que no puedes hacer a escala sino que tienes que decidir A quién primero y le vas a mirar y así vas a hacerlo de manera consciente y o sea de manera específica No porque no lo puedes aplicar a nivel global es a eso Por dónde iba de este tipo de técnicas que sería mejor que deshacerse de cifrado sí estamos hablando un poquito de que los que están a favor digamos de este de eliminar extremo en el

cifrado extremo extremo pues podrían utilizar estas técnicas para apoderarse de la información no los que no no los que están a favor no los que están en contra o sea yo estando en contra digo Oye tienes estos mecanismos es algo que un exploit que tú le vas a aplicar no puedes aplicarlo a todos los ciudadanos del mundo que es exactamente lo que queremos aplicalo solo a la persona que se lo tienes que aplicar perfecto Oye palante pero sitúa todo nos quitas la privacidad entonces claro es algo pasivo es como ya nadie tiene privacidad ya nosotros nos encargamos de mirar a quien nos interés Sí el único tema que igual dirían no a esto porque es bastante No complicado sino Supongo que les gustaría algo en plan cero clic en plan yo no tengo yo no tengo ganas de comprometer o no quiero arriesgarme a comprometer el dispositivo de un usuario evidentemente pero ahí tenemos claro yo por un parte quizá volviendo también al debate de antes evidentemente Esta técnica específicamente ya hemos determinado que no es académica no por eso yo hablaba de este tipo de tecnologías pero ahí tenemos la base de datos de fotos conocidas de pornografía infantil que utilizan los hashes para detectar si alguien tiene eso en el móvil sin tener que tener la foto en sí solo mirar la firma digital Claro si nosotros el hecho de que haya protecciones como el cifrado extremo extremo lleva a innovar y encontrar maneras de poder aún así luchar no contra la pornografía infantil o otras cosas pero si de repente decimos No mejor no nos vamos a poner aquí a innovar a gastar tiempo vamos Mejor a quitarle la seguridad a todo el mundo y así ya todo es transparente y ya está quizá los siguientes que vivamos en casas de cristal y entonces así pues también Mira más fácil no Pues por eso decía lo de activo ya lo están haciendo un poco vendiendo tantos cacharros que tenemos en casa no como todos estos cacharros inteligentes no que la gente se acostumbra a los asistentes de casa que vamos que estamos traqueados por todos lados y los gobiernos podrían abusar de esto Sí pero bueno por lo menos eso sí sí por lo menos eso es de manera consciente tú lo compras No un poco Sabiendo lo que hay o no Bueno la educación Pero sí bastante interesante Sí pues bueno queridos oyentes como siempre Hemos llegado hasta el final un episodio un poco más largo incluyó debate eso es de lo que se trata educación divulgación y sobre todo que vosotros formáis vuestra propia opinión que es de lo que se trata y tengamos aquí un poco de debate y diversión Así que dejarnos saber lo que opináis contestar a la pregunta del episodio dejarnos review si te gusta este episodio parece que el anterior ha gustado un montón pues déjanos reviews ahí donde nos estés escuchando que no te cuesta nada un comentario nos ayuda un montón Muchas gracias y por apoyarnos ahí online y nada por darnos ganas de seguir con estos episodios este bastante conspiranoico pero Esperamos que os haya gustado bueno tampoco yo me estaba rasgando en todo lo que había quizás cadena queridos oyentes que estamos a cinco de los 100 quedaros con nosotros Muchas gracias por todo Adiós adiós chao chao si te ha gustado este episodio y quieres ayudarnos a seguir con el podcast compártelo con tus amigos y compañeros con tu apoyo podremos atraer y despertar el interés por la ciberseguridad de mucha más gente Acuérdate de dejarnos un comentario y una valoración donde nos estés escuchando también puedes seguirnos en Twitter Instagram y Facebook te esperamos en el próximo episodio de tierra de Harris