Global Encryption Day – October 21 2024 - Encrypt Today to Safeguard Tomorrow: The Encryption Summit

Artículo 45 de eIDAS: Detrás de las Escenas

Robin Wilton - Internet Society: Miren el eIDAS, Artículo 45, un tema que estoy seguro está en la mente de todos. Si no han oído hablar del Artículo 45, no se preocupen. Lo abordaremos muy pronto. Pero antes de eso, tengo algunas notas administrativas. Primero, estas sesiones tienen un código de conducta.

Así que asegúrate de estar al tanto de eso para evitar cualquier sorpresa desagradable para cualquiera. En segundo lugar, tenemos una función de chat y una función de preguntas y respuestas. Por favor, envía tus preguntas a través de una de esas opciones. Y por último, la interpretación está disponible en francés, español y portugués. Deberías ver un ícono de globo en la parte inferior de tu pantalla en Zoom para activar la función de interpretación si la necesitas.

Eso es todo en cuanto a los avisos. Tenemos 50 minutos para esta sesión, lo cual no parecerá suficiente, así que no voy a gastar tiempo dándoles mini biografías de todos los ponentes. Basta con decir que vale la pena buscar sus biografías en línea porque hemos logrado reunir un conjunto increíble de expertos en la materia para esto.

Muy brevemente, ellos son Alexis Hancock del proyecto CertBot de la EFF, donde es la directora de ingeniería. Dennis Jackson de Mozilla, donde está en el equipo de ingeniería criptográfica, y por eso me refiero a encriptación, no criptomonedas. Y Thomas Lohninger, quien es el director ejecutivo de Epicenter. Así que bienvenidos a mi panel.

Bienvenidos a todos en la audiencia. Esperamos tener una sesión fascinante. Para poner el contexto a un nivel muy general, el Artículo 45 define parte de una estrategia general de la Unión Europea con respecto a la identificación digital como parte de una iniciativa más amplia llamada eIDAS. El enfoque principal de eIDAS ha sido históricamente una identidad digital para el ciudadano, y ha evolucionado para incluir funcionalidades similares a una billetera o, en principio, afirmaciones confiables.

de atributos individuales, como identidad, edad, cualificaciones profesionales, etc. De lo que estamos aquí para hablar hoy es de una parte muy específica de eso, el Artículo 55 de las regulaciones de IDS. Y, creo, Thomas, voy a dirigirme a ti primero, si me permites, para que amplíes esa imagen muy básica que di con una pequeña explicación de lo que es el Artículo 45, si puedes, y luego quizás continuemos con algunas de las características más amplias del eIDAS como esquema.

Thomas Lohninger - epicenter.works: Muy contento de hacerlo. Gracias, Robin. Espero que todos puedan escucharme bien. Sí, el reglamento eIDAS es en realidad una pieza de legislación muy antigua. Fue adoptado por primera vez en 2014. Y la misión principal de esta ley europea es establecer una plataforma armonizada para la identidad digital. Esta ley de 2014 nunca se materializó completamente porque había razones por las cuales los estados miembros nacionales, los estados miembros de la UE, no querían básicamente reconocer todos los diferentes sistemas de identidad digital de otros países. Y así, en junio de 2021, la Unión Europea comenzó a reformar este reglamento eIDAS, y básicamente contenía dos grandes proyectos. Uno era la llamada Cartera de Identidad Digital Europea, que debería realmente establecer un sistema armonizado para identificar a personas físicas y jurídicas, como personas y empresas, frente al sector público y privado, en línea y fuera de línea y en proximidad física, y también permitir la verificación de atributos sobre estas personas, en línea y fuera de línea. Y esto, lo que es importante, también está destinado a ser un sistema universal de propósito general.

Entonces, realmente debería abarcar desde licencias de conducir, euros digitales, controles fronterizos, todos los diferentes tipos de sociedad, incluso visitas al médico. Todo se basará en esta billetera de identidad digital europea. Y la segunda parte de esta reforma fue Quox, el Artículo 45, que nos trae aquí hoy, donde esta idea de querer tener a todos identificados, también se extiende a los sitios web.

Y, como pronto explicaremos más a fondo, estableció esta idea de que los propietarios, las personas detrás de un sitio web, sean autenticados hacia los usuarios que están usando o visitando un sitio web. Y así, esta idea de tener la propiedad del dominio identificada con un certificado que los proveedores de navegadores también están obligados a mostrar a sus usuarios es, en cierto modo, una idea antigua, pero una idea que la Unión Europea quiere volver a poner sobre la mesa, tal vez para entrar en algunos de los argumentos que hemos escuchado en el debate, por qué algunos de los estados miembros piensan que es una buena idea.

Nosotros, en Epicenter Works, hemos estado trabajando en esta reforma desde el primer día. Debo decir que nuestro enfoque principal era la billetera, porque como una ONG de privacidad, eso era algo donde vemos un ataque drástico a la anonimidad en línea, a nuestros datos de identidad verificados criptográficamente en el gobierno, certificados, siendo proliferados a áreas donde realmente no deberían estar, como las grandes tecnológicas o las agencias de calificación crediticia, pero también estábamos igualmente preocupados por el Artículo 45 y este ataque a la arquitectura de confianza de la World Wide Web. Y creo que lo dejaré ahí.

Robin Wilton - Internet Society: Gracias. esos 5 euros que te di por la transición perfecta fueron bien gastados. porque creo que donde lo dejaste fue, sí, hay estas posibles implicaciones de privacidad al tener, lo que en la práctica puede ser una identidad emitida por el gobierno central que se usa como base para todas estas afirmaciones a nivel de atributos y creo que volveremos a eso a su debido tiempo. Pero donde lo dejaste fue, está esta idea de identificar sitios web para el usuario final también. y entonces Alexis, creo que me gustaría dirigirme a ti a continuación, si puedo. La idea de identificar sitios web para el usuario, esto suena familiar porque hemos tenido el pequeño candado en el navegador por un tiempo, y luego hemos tenido la barra de URL poniéndose verde para decirte que este sitio web realmente es, realmente, es el que pensabas que ibas a visitar. ¿Estamos reinventando eso?

Alexis Hancock - EFF: Sí, esto fue una repetición. No hay otra manera elocuente de decirlo, donde teníamos certificados de validación extendida y abordamos esta idea de verificar tu identidad a través de TLS, que era un enfoque que ya habíamos tomado antes.

Y no cumplió con las promesas que alguna vez tuvo sobre poder atraer al usuario final en un sitio web para que no solo se sintiera seguro, sino que también pudiera saber que la persona o entidad detrás del sitio web es quien dice ser, utilizando TLS para hacerlo a través de certificados de validación extendida.

Cuando se propusieron los certificados de validación extendida, estábamos en una época diferente. La web no estaba tan encriptada. La web era menos segura y teníamos un ecosistema donde los certificados de validación de dominio no estaban tan automatizados y no se extendían tanto al usuario web cotidiano y al sistema empresarial que tenemos hoy.

Poder automatizar estas cosas y poder automatizar la seguridad para los servicios web, los servicios que existen. Así que tenemos certificados EV. Y pasamos por ese ciclo y alrededor de 2018, creo que los navegadores en gran medida decidieron deprecar la interfaz de usuario del candado verde porque no estaba logrando lo que se proponía.

Originalmente, fue un gran esfuerzo. Y quiero señalar que los certificados EV no son baratos. Son caros en comparación con los certificados de validación de dominio. Y realmente fue la emisión de certificados de validación de dominio lo que ayudó a que la

web se volviera más encriptada. Más que los certificados más caros y más engorrosos como la validación extendida.

Entonces pasamos por este ciclo. Y cuando vi esto, vi una repetición de una solución a un problema que no cumplió con los estándares que se propuso alcanzar.

Robin Wilton - Internet Society: Interesante. Bien. Entonces, los temas que creo que estamos abordando son, como dijiste, TLS, seguridad de la capa de transporte, que proporciona confidencialidad.

para las sesiones del navegador, siempre que tengas un medio seguro de intercambio de claves entre el servidor y el navegador, pero ese medio seguro de intercambio de claves en sí mismo significa que necesitas identificar correctamente el servidor, de lo contrario, podría estar obteniendo una sesión segura desde mi navegador, pero podría no ser con el servidor web correcto.

Entonces, como dices, TLS resuelve ese problema técnicamente. Pero luego tienes ese paso procedimental de, ¿es esa la clave pública del sitio web propiedad de la organización que dice ser dueña del sitio web? Y creo que es ese paso procedimental. Entonces, Dennis, ¿puedo consultarte sobre este punto?

Porque. y tú has estado involucrado tanto en la tecnología de cifrado de sesiones entre navegadores y sitios web, pero creo que tú y tus colegas también han trabajado en esta idea de la transparencia de certificados. Entonces, ¿cómo detectas el mal comportamiento entre los propietarios de certificados de sitios web?

Supongo que la pregunta que quiero resumir es si quieres decirle a alguien que este sitio web está usando un certificado falso para afirmar que no es quien dice ser. ¿Es el usuario final la persona adecuada para decírselo?

Dennis Jackson - Mozilla: Gracias, Robin. Sí, creo que es una pregunta muy interesante. Entonces, desde la perspectiva del usuario final en el navegador, como agente de usuario, tenemos que tomar una decisión sobre si las claves que vemos, el certificado que vemos, es uno de confianza, es el confiable para ese sitio web en particular.

Y creo que, como mencionaste, aunque podemos tomar algunas decisiones técnicas al respecto, en última instancia, el usuario nunca estará en una posición de estar completamente informado sobre ese sitio web y sus prácticas y políticas particulares, y de poder entender si ese sitio web es la pieza correcta de información de autenticación para esta conexión en particular.

En los días de los certificados EV, como mencionó Alexis, pensamos que tal vez agregar más información a ese certificado podría ser una forma de ayudar a los usuarios a

tomar esta decisión, y como mencionó Alexis, realmente no fue una estrategia exitosa. Así que lo que ha sucedido en su lugar es que nos hemos movido más hacia un sistema de transparencia pública.

Y ahora, cuando las autoridades de certificación emiten los certificados que se utilizan en TLS, deben ser registrados públicamente con varios operadores de registros de transparencia. Y el valor de esto es que estos registros ahora son accesibles públicamente. En particular, el propietario del sitio web, un investigador de seguridad o cualquier otra persona puede inspeccionar estos registros y revisar los certificados que se han emitido.

Y en particular, en el caso del propietario del sitio web, pueden decir, reconozco este certificado y esta clave pública porque son míos. Yo los generé, los solicité y, por lo tanto, son seguros. Pero si ven algo que no solicitaron, algo que no les pertenece pero que se está utilizando para respaldar una conexión a su sitio web, pueden reportarlo como un problema serio y, en última instancia, tomar medidas en base a eso para asegurar las conexiones a su sitio web.

Robin Wilton - Internet Society: Mientras que eso, sería, eso es algo que el individuo realmente no puede hacer. Así que sí, decirles que está mal cuando no tienen los medios para hacer algo al respecto. Puede terminar frustrando a la gente. Dicho esto, me pregunto cuántas personas en la audiencia han visto una advertencia de certificado aparecer en su navegador que dice, Oh, este certificado del sitio web puede ser inválido.

¿Y cuántas personas realmente retroceden o intentan hacer algo al respecto en lugar de simplemente hacer clic y decir, ah, quería llegar allí de todos modos? Y sospecho que la gran mayoría probablemente caería en esa última categoría. Thomas, quiero volver contigo aquí porque Dennis mencionó prácticas y políticas de sitios web.

En otras palabras, ¿qué se necesita además de la tecnología para tener algún nivel de garantía de que el certificado de un sitio web realmente pertenece a esa organización? y Alexis habló un poco antes sobre los certificados EV, que implican, por ejemplo, que alguien de la organización proporcione una prueba de identidad mucho más sólida y prueba de su rol en la organización para obtener ese certificado.

Pero, la parte específica sobre la que quería preguntarte, y esto se acerca mucho más al Artículo 45, es ¿cuál es la diferencia entre los certificados previstos por el Artículo 45, estos llamados QWACs, Certificados de Autenticación Web Calificados, y los certificados TLS que mencionó Alexis, que después de todo son la base para esa sesión encriptada entre tu navegador y el sitio web?

Thomas Lohninger - epicenter.works: Gracias, Robin. Esa es una gran pregunta y, de hecho, una que hemos discutido extensamente en los tres años y medio desde que se propuso esta ley. Y, escucharías cosas diferentes de los legisladores y también de los

proveedores de servicios de confianza, que son las empresas que se beneficiarían económicamente del Artículo 45.

Y algunos de ellos dirían que son realmente dos cosas diferentes. Los quarks son simplemente otra palabra para los Certificados de Validación Extendida (EV) que están destinados a identificar al propietario de un sitio web y mostrarse a los usuarios, y sigue esta idea europea de que todo debe ser identificado. Tenemos un fuerte impulso en varias legislaciones sectoriales como la Ley de Servicios Digitales, donde la verificación de edad es un tema importante.

El espacio europeo de datos de salud, lo ves aparecer en todas partes estos días, parece que la UE está bastante decidida a erradicar el anonimato en línea, lo cual vemos como un gran problema. Y, por cierto, también tenemos un derecho a la seudonimidad en eIDAS en el Artículo 5 que intenta mitigar ese riesgo.

Y el Artículo 45, por supuesto, tiene una función dual. Así que algunas personas, y pudimos convencer a la mayoría en el Parlamento Europeo de seguir esa interpretación, que los QUOX no son certificados TLS. Los QUOX deben ser separados. Los QUOX deben encargarse solo de la identificación y separar la encriptación de extremo a extremo a través de TLS del certificado QUOX sería el camino correcto a seguir.

en el consejo, así que cuando los 27 nuevos estados miembros tuvieron que llegar a un acuerdo sobre esta ley, esta distinción no era tan clara. Y, los proveedores de servicios de confianza suelen estar bastante cerca de su gobierno, estas son organizaciones nacionales. Hubo un impulso para que los proveedores de servicios de confianza fueran reconocidos por todos los proveedores de navegadores.

Y a veces escuchabas argumentos como, sí, pero es tan engorroso entrar en la lista de Apple o Google o cualquier proveedor de navegadores y su almacén de certificados raíz. Y si el gobierno dice que es seguro y es lo suficientemente seguro para el estado, entonces también debe ser lo suficientemente seguro para estas grandes empresas tecnológicas.

Ese es un argumento que escuchamos mucho en las negociaciones. Y para volver a donde estamos legalmente, en mayo de este año, la Unión Europea aprobó el reglamento eIDAS y ya está en vigor. Pero hay los llamados actos de implementación que detallan las obligaciones en la ley.

Y también hay un acto de implementación sobre el Artículo 45, pero no lo hemos visto. En total, hay alrededor de 28. al menos 28 Actos de Implementación, a veces se pueden ver varios para una sola disposición legal y solo cinco han estado en consulta hasta ahora. La consulta terminó a principios de septiembre y, de hecho, mañana será la votación sobre esos cinco que solo conciernen a la billetera.

De hecho, hemos estado trabajando en eso muy de cerca y parece que podrían fracasar. Puedes leer en medios políticos y alemanes que hay un gran frenesí entre los estados miembros sobre si esos cinco actos de implementación siquiera se aprobarán. Y eso significa que esperaremos bastante tiempo hasta obtener los detalles técnicos sobre cómo se implementan los quarks y, Etsy, que es una organización de estándares que también trabaja en parte en torno a la vigilancia.

los estándares y la interceptación legal también tienen un lugar en la mesa y estas especificaciones técnicas. Así que la última palabra definitivamente no está aquí, pero es realmente bueno que podamos tener esta discusión.

Robin Wilton - Internet Society: Creo que nos has dado una visión realmente importante detrás del telón porque estoy seguro de que no es una coincidencia que hayas mencionado 28 actos de implementación diferentes para esto.

Y ese número parece coincidir, casualmente, con el número de estados miembros de la UE, con una diferencia de uno o dos, lamentablemente hablando. Lo han entendido, creo, porque también dijiste que has escuchado el argumento de que si esto es lo suficientemente seguro para satisfacer al gobierno, entonces debería estar bien para el ciudadano.

Y sin embargo, entre esos más de 20 estados miembros, vemos gobiernos de muy diferentes y complejas orientaciones políticas. Entonces, lo que realmente estás diciendo es que, por un lado, tenemos este conjunto global de reglas sobre cómo los certificados TLS entran en la lista de confianza de los principales navegadores. Y por otro lado, queremos posiblemente hasta 27 reglas nacionales diferentes sobre cómo estos certificados entran en la misma lista.

Y eso me parece ser el núcleo absoluto de este problema. Así que, con eso, Alexis, ¿puedo dirigirme a ti un momento? Hemos insinuado la idea de que hay un conjunto de reglas a través de las cuales los certificados TLS se integran en los navegadores. Y como dijo Dennis, esos a su vez dependen de políticas y procedimientos sobre cómo las autoridades de certificación asignan y certifican esos certificados.

¿Son estas las mismas reglas para los certificados QOX? Porque no suena así.

Alexis Hancock - EFF: Entonces no, y quiero analizar esto desde la perspectiva de un incidente de seguridad con un certificado emitido de manera incorrecta o malintencionada. Hace algunos años, Kazajistán, el gobierno básicamente había estado colocando un certificado para espiar el tráfico de sus ciudadanos.

Y lo hicieron a nivel del navegador, porque anteriormente eran de confianza. Y una vez que Mozilla se enteró, una vez que Chrome se enteró, dejaron de ser confiables porque no solo estaban actuando fuera del ámbito de los derechos civiles en general, sino que

también estaban actuando mal como una autoridad certificadora. Eso no es algo que se supone que debe hacer una autoridad de certificación.

Y una parte de eso es poder actuar rápidamente. Así que una vez que la gente se dio cuenta de lo que estaba pasando desde el nivel de monitoreo, se eliminó la CA y el certificado de Kazajistán y se les dejó de confiar. Cuando introduces la ley en ese proceso sin consultar a las partes involucradas, ralentiza significativamente la respuesta a incidentes de seguridad porque ahora los navegadores tendrían que pasar por un proceso legal solo para eliminar una CA o un QTSP si estaban actuando fuera de los límites.

Ahora hablemos de esos límites, ¿verdad? Entonces, tienes programas de Rootstore. Ahora, cada navegador importante tiene uno. Eso no siempre fue así. Siempre me gusta mencionar esto porque en esta conversación de los últimos tres años, se aborda TLS y se aborda G, se aborda el ecosistema como si fuera el mismo ecosistema que teníamos hace 10 años, y simplemente no es el caso.

Ahora tenemos programas de almacén raíz. Tenemos programas de almacén raíz que se comunican entre sí. Tienes líneas base, directrices. Tenemos transparencia de certificados. Tenemos controles de cuenta más estrictos. Hay un montón de cosas que están sucediendo que son más útiles que antes. Así que ahora tienes programas de almacén raíz, sus reglas y su proceso de auditoría.

Y no solo almacenes raíz, sino que cualquiera que decida que una CA puede entrar ahí, sino un proceso real de poder monitorear, auditar, y un proceso transparente para expulsar esa CA si es necesario. Así que ya hay un proceso establecido detrás de eso. El QTSP con Quox y el Artículo 45 podrían eludir completamente ese proceso y obtener automáticamente la confianza en los almacenes raíz del navegador.

Así que ahora puedes ver dónde estaría la superposición en términos de democracia, transparencia, y cómo se ve eso cuando tienes, esencialmente, una CA patrocinada por el estado, en este caso, capaz de eludir ese tipo de reglas, y no solo eludir las reglas, sino también estar legalmente obligada a ser requerida en estos navegadores.

Y cuando los navegadores adoptan la postura de que una CA no cumple con sus estándares, ahora tenemos un proceso legal completamente nuevo al que adherirnos, solo para que esa CA sea desconfianza si algo fue emitido incorrectamente, mal manejado o introducido de manera nefasta.

Robin Wilton - Internet Society: Y así que, sí, y parte de tu temor es que ese proceso legal tomaría tiempo en desarrollarse, y en realidad, desde el punto de vista de la seguridad operativa, necesitas que ocurra mucho más rápido, en un plazo más corto.

Thomas, iré contigo y luego Dennis, tengo una pregunta para ti también.

Thomas Lohninger - epicenter.works: Bueno. Gracias, Alexis, por tocar este tema y tienes toda la razón. Hay algunos obstáculos adicionales que se crean por esto, pero también quiero hacer una distinción importante. Cuando miras los considerandos y el debate legal, lo que se vería como una razón para excluir a un proveedor de servicios de confianza del almacén de CA raíz es algo más como DIGI Notar, es decir, una brecha de seguridad en la CA. Pero si hubiera un caso de interceptación legal y un proveedor de servicios de confianza de un país, tomemos un país con un estado de derecho débil, como Hungría, emitiera un certificado, totalmente legal para propósitos de agencias de inteligencia, por ejemplo, entonces ni siquiera estoy seguro de cómo se clasificaría eso. Queríamos tener un lenguaje más fuerte en torno a la interceptación legal porque es una preocupación principal para nosotros.

Pero lamentablemente, eso no es algo donde veamos un lenguaje contundente en la ley.

Robin Wilton - Internet Society: Sí, pintas un panorama preocupante y quería volver contigo, Alexis, sobre esto, justo antes de pasar al punto de Dennis. Realmente, me parece que. Al incluir estas autoridades certificadoras mandatadas por el gobierno en la misma lista como si fueran equivalentes a las que entran a través del proceso de autoridad certificadora y navegador, no solo se abre la puerta a, como diste el ejemplo de Kazajistán, y no son los únicos, creo que Mauricio intentó lo mismo, de un gobierno tomando medidas para instalar un certificado raíz que le permitiría, para, para, para descifrar e interceptar todo el tráfico que entra y sale de ese país.

Pero hay otro tipo de daño también, ¿no es así? Que es que, si las autoridades de certificación están en la lista de raíces de confianza del navegador y manifiestamente no son de confianza. ¿Qué le hace eso a la confiabilidad de las otras autoridades de certificación que, hasta donde el usuario sabe, llegaron allí por el mismo proceso?

Entonces, ¿cuál es el impacto en cosas como TLS allí?

Alexis Hancock - EFF: Creo firmemente que es necesario crear políticas de Internet y tecnología en torno a los problemas del mañana en lugar de los problemas de hoy. No todos los miembros de la UE operan de la misma manera, como dijo Thomas. Algunos de los entes pueden estar actuando, tal vez no en línea con los mismos principios democráticos que otros estados miembros de la UE.

Entonces, tienes que verlo desde ese punto de vista, desde la perspectiva de poder crear políticas tecnológicas que no piensen solo en términos geopolíticos. Tienes que pensar en cómo es realmente Internet. Y es algo global. Es una comunidad de ciudadanos globales en Internet.

Y me gustaría pensar que cada vez que he escuchado a los gobiernos hablar sobre soberanía y crear barreras en Internet en torno a las fronteras geopolíticas, nunca me he sentido tranquilo después de escuchar esos términos y nomenclaturas en relación

con Internet. Porque si, una vez que empiezas a crear políticas en torno a ese aspecto y no piensas en un enfoque más global de los ciudadanos de Internet y quiénes interactúan con él, y no creas políticas que protejan a las personas mañana y no solo hoy.

No sabes quién estará en el poder mañana. Así que deberías hacer políticas tecnológicas pensando en quién estará en el poder mañana y crear esas salvaguardias. El Artículo 45 habría puesto en peligro esa salvaguardia de confianza. Definitivamente, especialmente si tuvieras diferentes partidos actuando de manera diferente dentro de los estados miembros de la UE.

¿Qué le pasaría a un usuario si tuviera un QTSP de Hungría en comparación con otro país? ¿Dónde podrían siquiera evaluar eso? Y creo que no deberíamos poner esa carga en los usuarios comunes para que lo evalúen. Depende de nosotros, como expertos, políticos y educadores en este tema, llegar a un acuerdo sobre cómo debería ser eso en lugar de dejar la carga en los usuarios para que descubran cómo se ve esa confianza en la web.

Robin Wilton - Internet Society: Sí. Y definitivamente vamos a necesitar volver a los impactos en la privacidad, el seudonimato y los derechos fundamentales de esto. Pero quiero volver a incluir a Dennis. Lo siento, Dennis, has estado esperando pacientemente. Así que hay un par de cosas que me encantaría que abordaras, si puedes. Y la primera sigue bastante bien lo que Alexis acaba de decir.

Entonces, una de las, una de las, una de las objeciones que recibí, hace un par de años cuando estaba investigando sobre factores de confianza en Internet, fue que, esta objeción a la implementación y despliegue del Artículo 45, objetar a ello era antidemocrático en el sentido de que aquí tenías una regulación, que había sido producida a través del proceso democrático, la Unión Europea.

Y por otro lado, tenías a un pequeño grupo de especialistas en autoridades certificadoras que decían, no, esto es una mala idea. No vamos a permitir que lo hagan. ¿Es esto realmente algo antidemocrático, o hay una justificación que considerar?

Dennis Jackson - Mozilla: Creo que, para responder a eso, realmente tenemos que desglosar cómo surgió el Artículo 45.

Y de vuelta, como mencionó Thomas, en el 21, hubo un proceso público para elaborar esta ley e identificar lo que podría necesitar hacer. Y el resultado principal de eso fue una sugerencia, un requisito de que los navegadores reconocieran estos certificados y los usaran para mostrar este tipo de información de identidad adicional.

Y Mozilla y Edry y muchos otros grupos se involucraron en este tema y hablaron sobre los méritos de los certificados EV frente a los certificados DV, y así sucesivamente. Y

hacia mediados del 20, perdón, a principios del 23, esta ley se encaminó hacia su finalización. Y en el proceso de la UE, eso significa entrar en el Trílogo, que es una serie de negociaciones finales a puerta cerrada para producir el texto final.

Y fue solo en este punto cuando el Artículo 45 comenzó a metastatizar y a tomar un carácter completamente nuevo. Y fue durante estas negociaciones privadas cuando se introdujo un nuevo texto para imponer estos requisitos a los proveedores de navegadores, para reconocer a los QTSPs de la UE, a las CAs de la UE, y para no eliminarlos a menos que los gobiernos de la UE estuvieran de acuerdo.

en términos de principios democráticos, este mismo texto se introdujo en privado, se acordó en privado y casi se convirtió en ley esencialmente a través de un proceso de cabildeo privado que no fue transparente para el público, y del cual los expertos y académicos en ciberseguridad simplemente no estaban al tanto ni pudieron participar.

Lo que sucedió como resultado de eso, como reacción a eso, fue que estas ONG, los fabricantes de navegadores, académicos y expertos en ciberseguridad se unieron para decir que esto está mal, que no es algo que deba hacerse, que no es algo que vaya a aportar valor a los ciudadanos europeos, y esencialmente pidieron al Parlamento Europeo que se opusiera.

Y, en última instancia, el Parlamento Europeo decidió atender ese llamado y optó por presionar para que se enmendara ese texto y cambiarlo en el último momento, literalmente días antes de que se publicara, para introducir nuevas salvaguardias que significarían que la ley se restringiría en su impacto y no requeriría que los fabricantes de navegadores confiaran en estas ACs basándose en un dictado gubernamental.

Robin Wilton - Internet Society: Joe ha puesto una pregunta en la sección de preguntas y respuestas, diciendo que, las enmiendas a este Artículo 25, que permiten tomar acciones urgentes de seguridad, permitiendo la adherencia a la mejor experiencia de usuario en seguridad. ¿Eso alivia la presión sobre algunos de los problemas aquí? Si no, ¿te gustaría ver más? Dennis, quiero darte la oportunidad de responder primero, y creo que Alexis, podrías tener algunas ideas al respecto.

También, Thomas, levanta la mano si quieres intervenir en eso. Así que Dennis, continúa por

Dennis Jackson - Mozilla: un segundo. Sí, entonces el resultado principal de estos cambios de última hora fue introducir una nueva excepción que dice que no hay obligación de reconocer a los charlatanes que contradiga los derechos de los fabricantes y distribuidores de navegadores para autenticar sitios web de la manera y medios según su criterio.

Y eso es fundamentalmente la salvaguardia esencial, que protege contra el abuso de gran parte de esto. Aunque los navegadores seguirán reconociendo a los charlatanes y mostrando esta información de identidad a los usuarios, esto no se extiende a las claves criptográficas contenidas en esos charlatanes y los proveedores de navegadores aún pueden usar sus propios procedimientos de seguridad para esto.

Así que creo que esto es, ya sabes, una salvaguardia esencial y poderosa, pero al igual que con la billetera, ahora tiene que implementarse en un Acto de Implementación y realizarse en un estándar técnico. Y parte de mi trabajo en Mozilla ha sido colaborar con Etsy en cómo se verán esos estándares técnicos.

Y un enfoque central de esto ha sido dividir el átomo, por así decirlo. Así que tomamos los estándares QAC existentes, donde la información de identidad y la información TLS están contenidas dentro del mismo certificado, y los dividimos en dos para que tengamos un certificado TLS, que está puramente bajo el control del navegador y utiliza las prácticas transparentes existentes que hemos usado durante los últimos 20 años.

Y luego el propio QAC, que contendrá información sobre el nombre de dominio del sitio web e información sobre la identidad legal del sitio web, pero no se utilizará para establecer estas conexiones encriptadas. Y ha sido un proceso muy largo, acordar estos estándares, y aún no está terminado, y como mencionó Thomas, podría no estar terminado por otros seis meses más, ya que continúan las disputas técnicas y legales, pero en gran medida ha aliviado la presión, y creo que se ha evitado el peor de los casos.

Robin Wilton - Internet Society: Thomas, parece que estamos pasando por un proceso paso a paso de describir lo que dice la regulación, lo que significa y cuáles son sus implicaciones. Parece que estamos muy lejos de los objetivos tipo El DAS que describimos al principio en términos de cosas como funciones de billetera, mayor confianza del usuario, porque, Dios mío, no tengo una gran sensación sobre eso a partir de esta discusión.

pero, para decirlo claramente, ¿el Artículo 45 cumple su propósito?

Thomas Lohninger - epicenter.works: No, no realmente. Pero la pregunta es, ¿qué propósito sirve? Y si el propósito es realmente crear confianza en la World Wide Web, entonces creo que estaba defectuoso desde el principio. Si el objetivo era socavar la arquitectura de seguridad web, entonces el veredicto aún está pendiente, pero en última instancia quiero retroceder mientras repasamos la cronología, qué pasó y cuándo, y puedo confirmar que las negociaciones del Trílogo fueron realmente un momento desastroso.

No es mi primera ley de la UE, llevo haciendo esto durante 10 años, por eso tengo canas. Y fue un momento bastante esperanzador cuando organizamos esta carta de 400 académicos y ONG que realmente logró llevar este tema finalmente a la atención

del público porque el IDAS es súper nerd. Es una ley muy técnica y complicada que se negoció en su mayoría sin mucha supervisión pública.

Creo que fuimos la única ONG que proporcionó análisis constantes de cada versión de la ley, incluidas las versiones no públicas que se discutieron en el juicio, para permitir un debate y escrutinio público sobre lo que realmente estaba sucediendo. Pero fue con esta gran carta que realmente pudimos asustar a los eurodiputados y a la presidencia del consejo para que volvieran a la mesa y nos dieran concesiones que nos permiten tener una oportunidad de lucha ahora en la aplicación.

Y, al menos, pudimos incluir algunas de las disposiciones fundamentales de privacidad en el texto legal y su ley realmente avanza muy lentamente. Así que, una vez que tienes algo como esto, generalmente dura una década. Eso significa el efecto real en la práctica, en los navegadores de las personas, en los teléfonos inteligentes de las personas, cuando vas al médico, al dentista, al supermercado o cruzas la frontera.

Danos dos o tres años más y entonces realmente lo verás porque los estados miembros tendrán que ofrecer toda la gama de estas nuevas tecnologías y todo lo que pueda impactar nuestras vidas diarias. El argumento que es nuestra métrica de éxito y que curiosamente también es el argumento político más fuerte con los legisladores es que un gran proyecto como el eIDAS se juzga en última instancia por la confianza que los ciudadanos depositan en él.

La confiabilidad del ecosistema que creamos, cuán resistente es contra actores malintencionados o fraudulentos que intentan abusar o socavar el sistema. Y esto sigue siendo algo a lo que debemos prestar mucha atención. Debemos estar muy atentos. Por eso estoy muy pendiente de cómo va la votación mañana.

Y en realidad espero que fracase. Espero que tengamos más tiempo y que la comisión tenga que volver a la mesa de diseño con algunas de estas cosas. El Acto de Implementación de eIDAS solo se propondrá, creo que fue alrededor de mayo del próximo año, así que todavía hay tiempo. Y la pregunta particular que hizo Joseph, se refiere al Considerando 65.

Y sí, hay un lenguaje suficientemente bueno, como mencioné antes, para manejar algo como una violación de seguridad de un proveedor de servicios justo con medidas de precaución por parte del proveedor del navegador. Tienen que notificar a la comisión, a las autoridades nacionales, pero pueden actuar. Cuando se trata de una interceptación legal, tal vez con una orden de silencio, dependiendo del país y las leyes nacionales, no estoy seguro.

Y no estoy tranquilo de que el Considerando 65 sea realmente una salvaguardia lo suficientemente significativa como para prevenir ese tipo de abuso.

Robin Wilton - Internet Society: Sí, fantástico. Una de mis preguntas favoritas cuando me muestran algo así y me dicen lo maravilloso que sería, es decir, muéstrame qué en este sistema realmente previene el abuso de la funcionalidad que estás describiendo.

y sí, creo que es una pregunta fructífera para hacer en este caso, pero quiero, nos quedan 10 minutos, y quiero usar parte de ese tiempo contigo, Alexis, si me permites. Entonces, ahí tenías a Thomas, que trabaja para una organización especializada en entender, comentar y tratar de influir en este tipo de legislación de la UE.

y es bastante difícil dentro de la UE. ¿Cómo es cuando empiezas a mirar las implicaciones transfronterizas de esto? ¿Cómo explicas, Alexis, a los legisladores fuera de los EE. UU. qué es un trílogo para empezar? ¿Qué tipo de problemas has encontrado allí?

Alexis Hancock - EFF: Sí, así que esta fue mi primera ronda aprendiendo las diferencias clave entre los comités, la comisión, los parlamentos, los trílogos.

Y como este es mi primer intento, las canas aún no han aparecido. pero estoy bastante seguro de que en unos pocos intentos más lo harán. tratando de entender esto en el contexto de cómo se ve, no solo en los EE. UU., sino en el extranjero, en general, en Internet. ¿Y cómo se ve esto para la red de confianza? Como alguien que trabaja.

Algo así como en una línea más neutral de poder presumir los beneficios de la seguridad TLS automatizada, que es donde esto captó mi atención, esto inhibe, esto obstaculiza realmente la capacidad de automatizar certificados TLS, al por mayor, y diferentes estructuras, especialmente estructuras que definitivamente lo necesitan, como en EIDIS, donde tienes billeteras digitales, necesitas poder actuar rápido, necesitas poder mantenerte al tanto de la seguridad de una manera, como nunca antes, si realmente quieres implementar una identidad digital a gran escala para alguien, necesitas poder tener un sistema de confianza que tenga sentido.

Y retroceder a un sistema de confianza a puntos de vista más arcaicos no tenía sentido para mí, y traducir eso fuera de los EE. UU. y ver cómo podría ser, no los EE. UU., no los EE. UU., la UE, pero también mirándolo en los EE. UU. donde también están considerando la identidad digital de muchas maneras diferentes.

Aún no está a nivel federal en nuestro país, pero diferentes estados ya han implementado licencias de conducir móviles. Quiero decir que un poco más de 20 estados han implementado licencias de conducir móviles y han implementado billeteras o han contratado con Apple y Google para usar sus billeteras en sus sistemas nativos, iOS y Android respectivamente.

Entonces, lo que tienes aquí es una posible influencia. Los EE. UU. miran al RGPD para muchos de los avances en privacidad de datos en torno a la legislación y la política, y

temía que si esto se aprobaba tal como está, la gente lo vería como un ejemplo en la UE, diciendo, está bien, miren, la UE ha logrado esto con el Artículo 45, tal vez deberíamos adoptar un lenguaje similar y hacer cumplir esto.

Ni siquiera sé cómo sería esto si alguien de otro país visitara un sitio web respaldado por QTSP y fuera potencialmente defraudado si se abusara de este sistema. ¿Cuáles son los medios para poder impugnar eso o obtener algún tipo de compensación o retribución por haber sido defraudado?

¿Qué fue eso? ¿Cómo se vería eso para alguien? Y hay muchas personas fuera de la UE que usan sitios basados en la UE. No se habría limitado solo a ese ecosistema de ser un ciudadano de la UE. Así que no estoy muy seguro de cómo se habría visto, pero poder explicar eso y, implorar a mis, los, políticos dentro de la UE diciendo que están dando el ejemplo, dieron el ejemplo con el GDPR, así que realmente necesitamos que hagan esto bien en este sentido, o al menos poder garantizar las ganancias básicas de seguridad aquí, que hemos obtenido en los últimos 10 años y no retroceder a una época en la que TLS era caro, oneroso, tú.

Y sinceramente, no tan estricto como solía ser, o como lo es ahora en cuanto a poder apoyar la automatización y apoyar la capacidad de, en realidad, automatizar la seguridad de una manera que tenga sentido para todos y permitir que los participantes en el ecosistema tomen las decisiones como lo hacen ahora, porque es un proceso transparente.

Es un proceso que está fuera de la UE, aunque tenemos miembros de la UE en diferentes organismos de estándares, ellos están tomando esas decisiones juntos. No es solo en un silo. Así que tomar esta decisión en un silo no tenía mucho sentido para mí. Y eso es lo que estaba tratando de explicar a las audiencias fuera de la UE, para que no necesariamente sigan ese camino en particular si sucediera.

Robin Wilton - Internet Society: Sí, y creo que podemos ver esto por analogía con otros productos y servicios, lo último que quieres es un navegador que solo funcione en la UE. Así no es como funcionan estas redes o los fabricantes de navegadores, teniendo que desarrollar productos diferentes para distintos mercados geográficos, eso realmente empieza a erosionar algunos de los beneficios fundamentales de tener una Internet global.

Bien, nos quedan solo unos minutos. Solo quiero, por así decirlo, dar una vuelta a la mesa para algunas reflexiones finales. Dennis, ¿eres optimista en este momento, desde un punto de vista técnico? Y luego, si la respuesta a eso es sí o no, ¿qué hay del optimismo no técnico?

Dennis Jackson - Mozilla: Creo que me describo como un optimista, pero me cuesta ser optimista sobre el proceso mediante el cual se ha llegado a esto y la forma en que se están redactando estas regulaciones y estándares técnicos.

Creo que, ya sabes, entonces hay

Robin Wilton - Internet Society: un poco de eso que es abierto y transparente y en el proceso democrático. Mencionaste, por ejemplo, que el Parlamento Europeo tomó el caso en contra de esto, pero antes de llegar a ese punto, también hubo sesiones a puerta cerrada más problemáticas.

Dennis Jackson - Mozilla: Sí, y creo que no solo antes de ese punto, sino también ahora después de ese punto, donde la Comisión finalmente redactará un Acto de Ejecución para realizar esto, basado en un estándar técnico, y ese estándar técnico se desarrollará a puertas cerradas en ETSI, lo cual requiere un tipo de acuerdo comercial extenso para contribuir.

No será una norma en la que cualquiera pueda opinar, o como en el ITF, donde tienes una norma más participativa, y ese Acto de Ejecución no será supervisado por el Parlamento. Fundamentalmente, dependerá del Consejo Europeo, de los estados miembros, decidir si lo consideran adecuado.

Y eso limita la oportunidad de escrutinio y control sobre estos procesos, y hace mucho más difícil que el ciudadano europeo promedio participe en este proceso de manera significativa. Y esa Europa

Robin Wilton - Internet Society: El Consejo, por supuesto, está compuesto por políticos nacionales. Sí. Entonces, Thomas, quizás puedas cerrar esto para nosotros con algunas reflexiones sobre el impacto más amplio de esto en cosas como el anonimato y el seudonimato y otros derechos fundamentales y la tecnología que los respalda.

Thomas Lohninger - epicenter.works: Sí, claro. Estoy de acuerdo con Dennis. Siempre digo que soy optimista por profesión. Y, de alguna manera, es bastante difícil ver las manos de nuestros gobiernos extendidas aquí frente a nosotros con las consecuencias devastadoras. Al mismo tiempo, hay razones para tener esperanza porque podríamos lograr cambios significativos en el proceso, en las negociaciones con la presión pública.

siempre y cuando nosotros, como un público informado, como expertos de la sociedad civil, nos incluyamos en estos procesos. Podemos marcar la diferencia. De hecho, en los actos de implementación que se votarán mañana, una cuarta parte de nuestras enmiendas fueron aceptadas por la comisión. Así que hay oportunidad de influir en estas decisiones si prestamos atención.

Ese escrutinio público es clave. Y estamos en un momento decisivo. Alexis mencionó cómo los sistemas de identidad digital ya están proliferando en muchos estados americanos. Soy parte de un proyecto de la ONU sobre infraestructura pública digital que se basa en el sistema ATAR de la India y en muchas otras regiones donde estos sistemas están surgiendo.

Así que creo que es precisamente el momento de prestar mucha atención y utilizar estas experiencias de otros países para aprender y tal vez no repetir los mismos errores. Y en cuanto al proceso concreto de eIDAS, hay una obligación legal de tener un período de consulta de cuatro semanas después de los actos de implementación del Artículo 45.

Así que hay una manera de tener un registro oficial de todas las contribuciones al respecto. Esa es una gran oportunidad para una campaña. Y, como alguien que tiene, no estoy seguro de cómo irá la votación mañana y el consejo es más difícil que el parlamento, pero al menos estamos en posición de bloquear estos actos de implementación.

Así que definitivamente hay una oportunidad y hay una razón para tener esperanza si todos hacemos nuestro trabajo y seguimos prestando mucha atención a estos temas tan técnicos. Todavía tengo la esperanza de que podamos llegar a un buen resultado y que estos grandes sistemas técnicos respeten nuestros derechos fundamentales.

Robin Wilton - Internet Society: Maravilloso. Mira, creo que hemos llenado nuestros 50 minutos con una discusión increíble.

Tengo algunos agradecimientos. Me encantaría agradecer a Seema Karaman y al equipo de Mozilla por organizar este taller y este panel, Thomas Loeninger, Dennis Jackson, Alexis Hancock. Como prometí, qué alineación fantástica de expertos en la materia. Muchas gracias por participar hoy, como parte del Día Global de la Encriptación.

Y gracias a todos los que se han conectado para escuchar, participar y enviar sus preguntas. Muchas gracias. Espero hablar con ustedes la próxima vez también.

Alexis Hancock - EFF: Gracias.

Robin Wilton - Internet Society: Gracias. Adiós. Gracias.