UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat d'Informàtica de Barcelona

Web tracking

Zhihan Lin, Manuel Liu Wang, Junjie Li

Index

1. Introducción

El web tracking se refiere al conjunto de técnicas y herramientas utilizadas para recopilar información sobre el comportamiento y las interacciones de los usuarios en la web. Esta práctica se ha extendido de manera significativa con el crecimiento exponencial del Internet y la digitalización de servicios, permitiendo a empresas y organizaciones:

- **Personalizar experiencias de usuario**: Mediante la recopilación de datos, es posible ofrecer contenido y publicidad adaptada a los intereses y comportamientos de cada individuo.

- **Optimizar campañas de marketing**: La información obtenida a través del tracking facilita la toma de decisiones en tiempo real y la mejora de estrategias publicitarias.

- **Analizar tendencias y comportamientos**: Permite a los analistas comprender patrones de uso, facilitando el desarrollo de productos y servicios que respondan a necesidades específicas.

Sin embargo, la adopción masiva de estas técnicas ha generado preocupaciones en torno a la privacidad, la seguridad de la información y el cumplimiento normativo. En un entorno donde la protección de datos es cada vez más crítica, se hace imprescindible estudiar el web tracking desde una perspectiva integral que contemple tanto sus beneficios como sus riesgos.

Este proyecto tiene como finalidad proporcionar un análisis del web tracking, abarcando desde sus aspectos históricos y técnicos hasta sus implicaciones éticas y legales. Entre los objetivos específicos se destacan:

- **Evolución y técnicas actuales**: Revisar la evolución histórica del web tracking y describir las tecnologías y metodologías empleadas en la actualidad (por ejemplo, cookies, fingerprinting, beacons, entre otras).

- **Análisis de desafíos y soluciones**: Identificar los principales problemas asociados al tracking, como la invasión a la privacidad y las dificultades en el cumplimiento normativo, y evaluar las soluciones y propuestas emergentes en el ámbito tecnológico.

- **Evaluación del impacto en el mercado**: Examinar el uso comercial del web tracking, su impacto en la publicidad digital y la distribución de contenidos multimedia, y las tendencias futuras en este campo.

El alcance de este proyecto se centra en un análisis teórico, abordando la parte técnica.

2. Estado del Arte

Este apartado ofrece una visión global y cronológica del desarrollo del web tracking, poniendo de relieve tanto su evolución histórica como las técnicas actuales y el marco normativo y ético que lo regula. Este análisis permite comprender cómo se han desarrollado las metodologías de seguimiento en la web y cuáles son los desafíos que han surgido a lo largo del tiempo.

2.1. Evolución Histórica

El web tracking ha experimentado un notable desarrollo desde sus inicios, transformándose conforme evoluciona el ecosistema digital:

- **Orígenes y Primeros Métodos**: En las primeras etapas de Internet, el seguimiento se limitaba a métodos básicos, como el análisis de logs de servidor y el uso rudimentario de cookies. Estas técnicas permitían identificar a los usuarios a través de sesiones temporales, facilitando el estudio del comportamiento en línea en un entorno mucho menos complejo.

- **Expansión y Diversificación**: Con el crecimiento exponencial de la web y el aumento del comercio electrónico, se intensificó la necesidad de técnicas más sofisticadas. A lo largo de los años 2000, las cookies se convirtieron en la herramienta predominante para el seguimiento, permitiendo personalizar la experiencia de navegación y optimizar campañas de marketing.

- **Avances en Tecnologías de Seguimiento**: El auge del big data y el análisis avanzado impulsó la incorporación de nuevas metodologías, como el fingerprinting del navegador, que combina múltiples parámetros (configuración del sistema, plugins, resoluciones de pantalla, etc.) para crear un identificador único, y el uso de beacons o píxeles de seguimiento, que permiten recoger datos de forma casi invisible para el usuario. Esta evolución ha ampliado el alcance y la precisión del seguimiento, pero también ha planteado nuevos desafíos en términos de privacidad y seguridad.

2.2. Técnicas y Tecnologías Actuales

En el escenario actual, el web tracking se sustenta en diversas técnicas que, en conjunto, permiten la recopilación y análisis de datos de los usuarios con un alto nivel de detalle. Una de las metodologías más extendidas es el uso de cookies, que son pequeños archivos de texto almacenados en el navegador. Originalmente diseñadas para gestionar sesiones y facilitar la experiencia de usuario en sitios web, las cookies han evolucionado hasta convertirse en herramientas fundamentales para la personalización de contenidos y la ejecución de campañas publicitarias dirigidas. Esta técnica permite rastrear la actividad del usuario a lo largo del tiempo, identificando patrones de comportamiento y preferencias, lo que se traduce en una mayor eficacia en la segmentación de audiencias.

Otra técnica avanzada es el fingerprinting, que se diferencia significativamente del uso de cookies en su capacidad para generar una "huella digital" única del dispositivo del usuario. El fingerprinting recopila información detallada sobre la configuración del navegador, el sistema operativo, la resolución de pantalla, los plugins instalados y otros parámetros técnicos. Al combinar estos datos, se puede identificar de manera precisa a un usuario incluso sin necesidad de almacenar información localmente. Este método, aunque extremadamente efectivo, plantea serias cuestiones de privacidad, ya que resulta casi imposible para el usuario desactivar o evitar su uso sin recurrir a herramientas especializadas.

Los beacons, también conocidos como píxeles de seguimiento, constituyen otra tecnología crucial en el web tracking. Estos son pequeños fragmentos de código o imágenes diminutas, invisibles para el usuario, que se integran en las páginas web y correos electrónicos. Al cargarse, estos beacons envían información de manera automática a los servidores de análisis, permitiendo medir interacciones como aperturas de emails o visitas a páginas, de forma casi imperceptible. Esta técnica es valorada por su capacidad para proporcionar datos en tiempo real sobre la interacción del usuario, facilitando una respuesta inmediata en estrategias de marketing digital.

Además, la evolución tecnológica ha permitido la integración de herramientas de análisis avanzadas que emplean algoritmos de machine learning para procesar grandes volúmenes de datos. Estas plataformas no solo almacenan y organizan la información recopilada mediante cookies, fingerprinting y beacons, sino que también son capaces de identificar patrones complejos y predecir comportamientos futuros. La capacidad de correlacionar datos provenientes de múltiples fuentes, incluso en entornos de Internet de las Cosas (IoT), ha llevado a que el web tracking se convierta en un elemento central para la toma de decisiones en tiempo real en el ámbito comercial y publicitario.

3. Cookies

Las cookies son archivos de texto pequeños que los sitios web envían a tu navegador para almacenar información sobre tu visita. Pueden guardar datos como tu nombre de usuario, preferencias o detalles de sesión, entre otros. Cuando regresas al mismo sitio, tu navegador reenvía estas cookies al servidor, lo que permite al sitio reconocer tu dispositivo y acceder a la información guardada previamente.
Las cookies cumplen diversas funciones, como mejorar la experiencia de navegación (mantener la sesión activa), adaptar el contenido mostrado (recomendar productos similares) o analizar el comportamiento del usuario (con fines publicitarios).

3.1. Funcionamiento

Las cookies funcionan principalmente en 4 pasos:

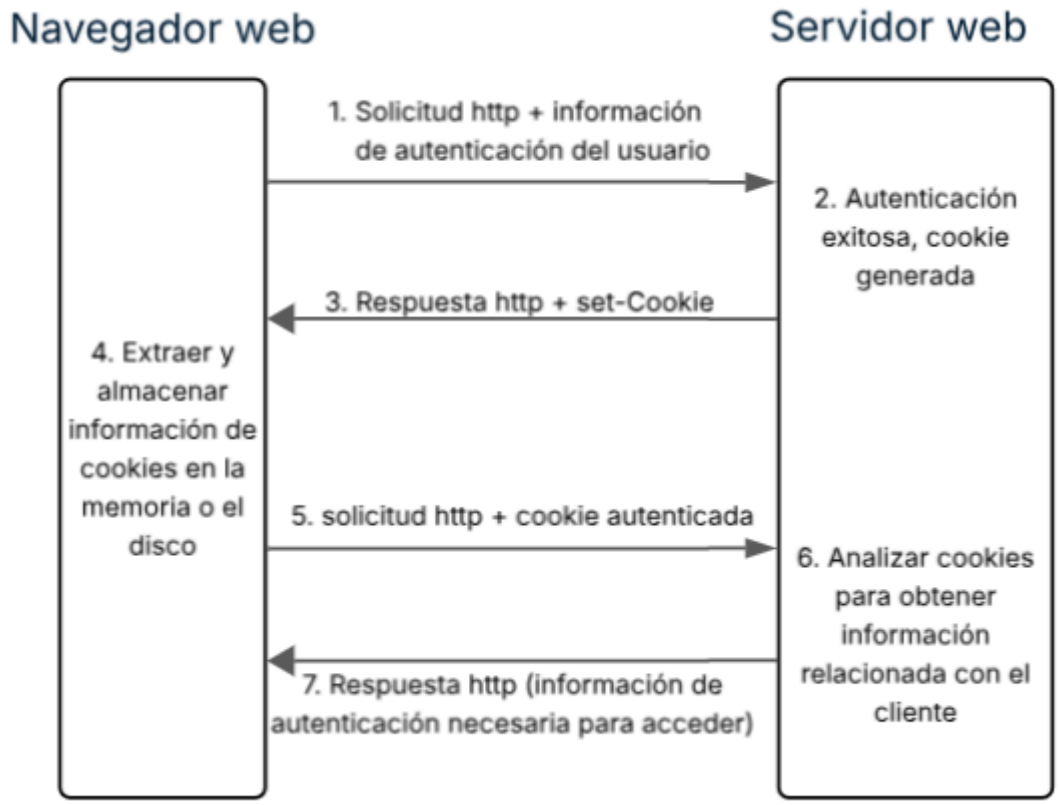
- **1) Envío de cookies:** Los sitios web envían cookies a tu navegador con información sobre tu visita.
- **2) Almacenamiento en el navegador:** Tu navegador guarda estas cookies.
- **3) Reenvío de cookies:** Cuando visitas de nuevo el sitio, el navegador envía de vuelta las cookies al servidor.
- **4) Recuperación de información:** El sitio web utiliza la información en las cookies para reconocerte y personalizar tu experiencia.

3.2. Tipos de cookies

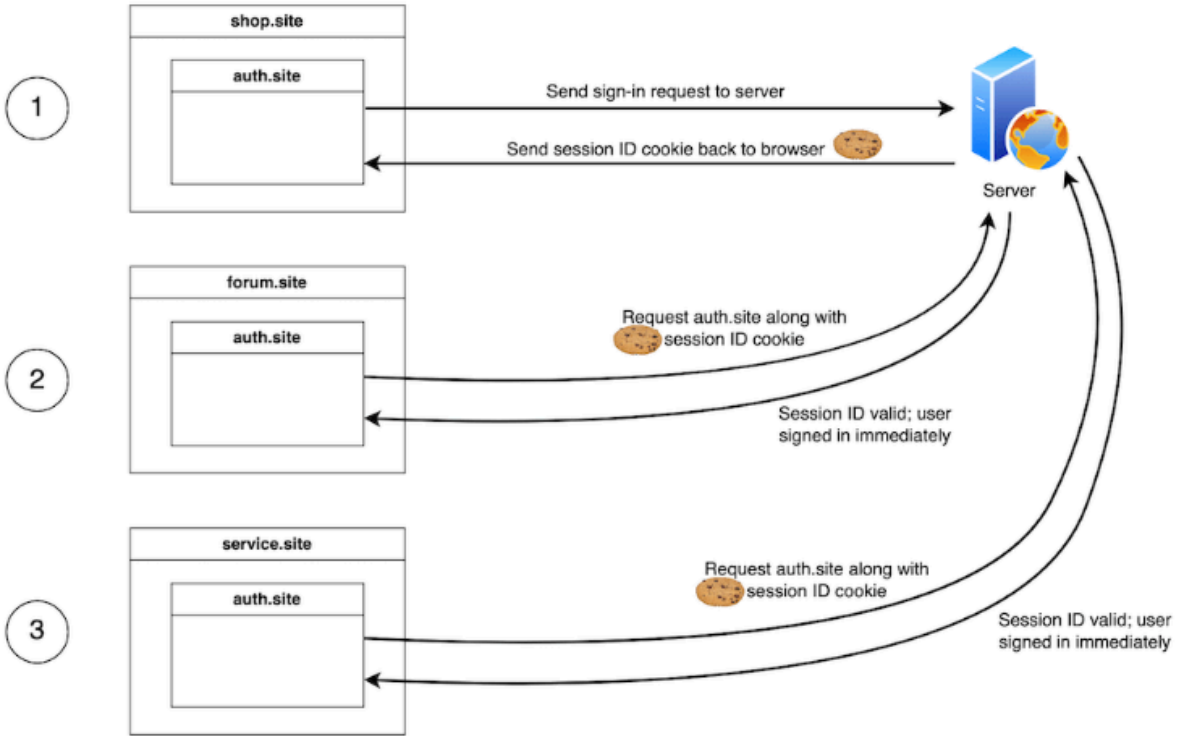
Existen varios tipos de cookies con características diferentes, las cookies de sesión son temporales y se borran cuando cierras el navegador. Sirven para mantener acciones como el carrito de compra o el inicio de sesión activo durante tu visita.
En cambio, las cookies persistentes permanecen en tu dispositivo por días, meses o incluso años, y se usan para recordar preferencias como el idioma o la configuración de una web.
Según su origen, las cookies propias son creadas por el sitio que visitas y se usan para funciones básicas como la seguridad o la autenticación.
Las cookies de terceros son colocadas por servicios externos como redes sociales o plataformas publicitarias, y sirven para rastrear tu comportamiento entre diferentes sitios web.
En cuanto a su finalidad, las cookies técnicas son esenciales para que una web funcione correctamente, como las que mantienen tu sesión segura en un banco online.
Las de preferencias guardan ajustes personales como el tema oscuro o la región, las analíticas recopilan datos sobre cómo usas el sitio, como las páginas que visitas o el tiempo que pasas en ellas. Por último, las cookies publicitarias registran tus intereses para mostrar anuncios personalizados basados en tu historial de navegación.
Algunas cookies requieren tu consentimiento según las leyes de privacidad, especialmente las de marketing y análisis avanzado, mientras que otras como las técnicas son necesarias y funcionan sin permiso. Los usuarios pueden gestionarlas desde la configuración de su navegador, aceptando, bloqueando o eliminando las que consideren oportunas.

3.3. Esquema

First-party cookie:



Third-party cookie:



4. Fingerprinting

El fingerprinting es un método avanzado de identificación y seguimiento de usuarios en internet que no depende de cookies ni archivos almacenados.
En lugar de eso, recopila y analiza múltiples características técnicas del dispositivo y navegador, como versión del sistema operativo, configuración de plugins, resolución de pantalla, zona horaria, fuentes instaladas y parámetros de hardware, para generar un identificador único de cada usuario.
Esta técnica es particularmente efectiva porque combina decenas de datos aparentemente inocuos que, al analizarse en conjunto, forman una "huella" digital prácticamente irrepetible.
A diferencia de las cookies tradicionales que pueden borrarse fácilmente, el fingerprinting persiste incluso cuando los usuarios limpian su historial o utilizan el modo incógnito, lo que lo convierte en un método más sigiloso y persistente para el rastreo online.
Su aplicación abarca desde la autenticación de seguridad avanzada hasta la publicidad dirigida y la prevención de fraudes, aunque también plantea importantes debates sobre privacidad dado que los usuarios generalmente no son conscientes de este tipo de recolección de datos.

4.1. Funcionamiento

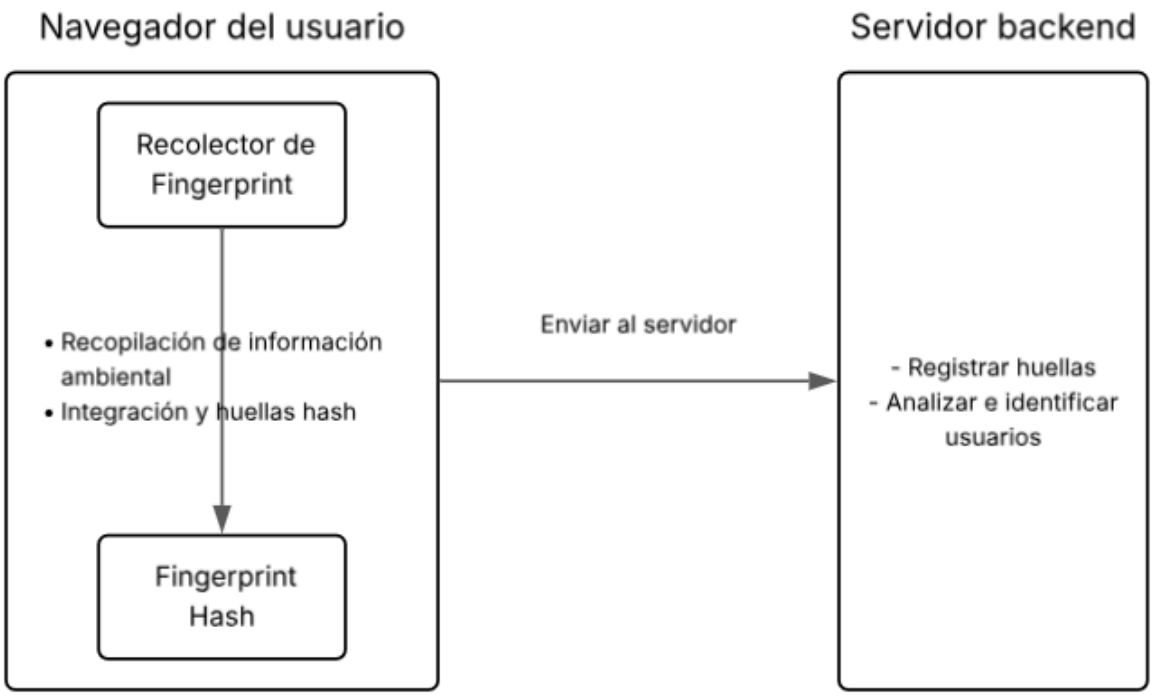
El fingerprinting funciona principalmente en 4 pasos:

- **1) Recopilación de datos:** Los sitios web utilizan scripts para recopilar información del navegador y dispositivo del usuario.
- **2) Creación de un perfil único:** Estos scripts recopilan datos como el tipo de navegador, sistema operativo, plugins instalados, resolución de pantalla, zona horaria, etc.
- **3) Asociación de la huella digital:** El sitio web asigna una "huella digital" única a cada perfil, lo que le permite identificar y rastrear al usuario.
- **4) Uso de la huella digital:** Los sitios web utilizan las huellas digitales para diversos fines, como publicidad personalizada, detección de fraude, análisis web y seguridad.

4.2. Tipos de fingerprinting

El fingerprinting de navegador consiste en recopilar datos específicos del navegador que usa una persona, como la versión, extensiones instaladas o configuraciones particulares, para crear un identificador único.
El fingerprinting de dispositivo se enfoca en características del hardware y software del equipo, como el sistema operativo, la resolución de pantalla o el modelo del dispositivo, generando una huella basada en estos atributos.
Por otro lado, el canvas fingerprinting aprovecha la tecnología HTML5 para dibujar elementos gráficos ocultos en el navegador, lo que revela diferencias sutiles en cómo se renderizan las imágenes, permitiendo distinguir a cada usuario de manera individual.

4.3. Esquema



5. Comparación de Alternativas

5.1. Análisis Comparativo de Técnicas:

Técnica	Eficacia	Invasión de Privacidad	Robustez Técnica
Cookies	Alta, pero fácilmente bloqueables o eliminables	Moderada; el usuario puede gestionarlas	Limitada por políticas del navegador y consentimiento legal
Fingerprinting	Muy alta; difícil de evadir	Alta; difícil de detectar y bloquear	Muy robusta; no depende de almacenamiento local

Análisis:
Las **cookies** permiten personalizar la experiencia del usuario mediante el almacenamiento de información local, como preferencias o identificadores de sesión. Son ampliamente

compatibles y fáciles de implementar, pero también fáciles de eliminar o bloquear con herramientas comunes de privacidad, lo que reduce su fiabilidad para el seguimiento persistente.

En contraste, el **fingerprinting** genera un perfil único del usuario basado en características técnicas del navegador y del dispositivo. Esta técnica es mucho más resistente a bloqueos, ya que no requiere almacenamiento en el cliente. Sin embargo, plantea serias preocupaciones éticas y legales, ya que es altamente invasiva y difícil de detectar por los usuarios.

5.2. Ventajas y Desventajas

5.2.1. Cookies

Ventajas:

- Fácil implementación y uso generalizado.
- Compatibilidad amplia entre navegadores y plataformas.
- Gestión transparente por parte del usuario (pueden aceptar o rechazar).
- Permiten personalización del contenido y sesiones persistentes.
- Requieren consentimiento, lo cual las hace más alineadas con normativas como el RGPD.

Desventajas:

- Fáciles de eliminar o bloquear, lo que reduce su fiabilidad.
- Dependientes del cliente (almacenamiento local).
- Sujetos a restricciones legales (RGPD, ePrivacy).
- Vulnerables al uso malintencionado si no se regulan adecuadamente.

5.2.2. Fingerprinting

Ventajas:

- Alta precisión para identificar usuarios únicos.
- Difícil de evadir, incluso con modos privados/incógnito.
- No requiere almacenamiento local ni intervención del usuario.
- Útil en entornos de alta seguridad (prevención de fraude, autenticación pasiva).

Desventajas:

- Considerada altamente intrusiva en términos de privacidad.
- Difícil cumplimiento con regulaciones de consentimiento y transparencia.
- Opuesta al principio de "privacy by design", difícil de auditar o gestionar por el usuario.
- Puede erosionar la confianza del usuario si no se informa adecuadamente.

5.3. Casos de Uso y Aplicaciones Prácticas

En esta sección se presentan los usos típicos de las **cookies** y el **fingerprinting** (huella digital del navegador/dispositivo) en los sistemas web modernos, destacando su valor en la funcionalidad, seguridad y experiencia de usuario.

5.3.1 Cookies

Las cookies son archivos de texto pequeños almacenados en el dispositivo del usuario por el navegador, y se utilizan comúnmente para mantener el estado entre el usuario y el sitio web. Sus aplicaciones principales incluyen:

- **Publicidad dirigida y perfiles de usuario**
    - Las cookies permiten rastrear el comportamiento de navegación del usuario entre diferentes sitios web.
    - Las plataformas publicitarias utilizan esta información para construir perfiles y mostrar anuncios personalizados.
    - Ejemplos incluyen Google Ads y Facebook Pixel.
- **Carritos de compra y gestión de sesiones**
    - En sitios de comercio electrónico, las cookies permiten conservar los productos añadidos al carrito incluso si el usuario cierra el navegador.
    - Las cookies de sesión también mantienen al usuario autenticado sin necesidad de iniciar sesión constantemente.
- **Preferencias del usuario y configuración personalizada**
    - Almacenan configuraciones como el idioma, el tema (oscuro o claro), el tamaño de fuente, etc.
    - Mejoran la experiencia del usuario al evitar tener que restablecer estas preferencias en cada visita.
- **Análisis estadístico y seguimiento de comportamiento**
    - Herramientas de análisis (como Google Analytics) utilizan cookies para recopilar métricas de tráfico, tiempo de permanencia, páginas visitadas, etc., con el fin de optimizar el contenido y la estructura del sitio.
- **Gestión del consentimiento y cumplimiento normativo**
    - Las normativas como GDPR (Europa) o CCPA (California) exigen el uso de sistemas de gestión de consentimiento para las cookies.

- Algunas cookies (por ejemplo, de análisis o publicidad) solo pueden activarse con el consentimiento explícito del usuario.

5.3.2 Fingerprinting

El fingerprinting es una técnica que recopila características del dispositivo del usuario (como el navegador, resolución de pantalla, fuentes instaladas, plugins, sistema operativo, etc.) para generar un identificador único, sin necesidad de usar cookies. Sus principales aplicaciones incluyen:

- **Detección de fraudes y protección de seguridad**
  - En contextos de alto riesgo como servicios financieros o comercio electrónico, permite identificar suplantaciones de identidad, uso compartido de cuentas o accesos desde dispositivos sospechosos.
  - El sistema puede detectar si un acceso proviene de un "nuevo dispositivo" o si hay un "comportamiento anómalo".

- **Autenticación pasiva y verificación silenciosa**

  - Facilita la autenticación sin requerir interacción constante del usuario, mejorando la experiencia.
  - Por ejemplo, combina ubicación, tipo de dispositivo y patrones de uso para verificar si quien accede es el propietario legítimo de la cuenta.

- **Limitación de bots y tráfico automatizado**

  - Permite identificar y bloquear bots sin necesidad de usar CAPTCHA.
  - Analiza la coherencia de la huella digital y el patrón de interacción para detectar tráfico no humano.

- **Seguimiento entre sitios (uso controvertido)**

  - Algunas plataformas usan fingerprinting para rastrear usuarios incluso cuando bloquean cookies, lo que genera preocupaciones de privacidad.
  - Dado que es difícil de detectar o bloquear, su uso está cada vez más regulado.

5.3.3 Elección Tecnológica y Consideraciones de Cumplimiento

- En **contextos donde se requiere el consentimiento explícito del usuario (como en la UE bajo GDPR)**, se recomienda priorizar el uso de cookies con mecanismos de transparencia y gestión de consentimiento adecuados.

- En **escenarios que requieren alta seguridad o presentan riesgo de fraude (como sistemas bancarios o antifraude)**, el fingerprinting puede ser más efectivo, aunque debe usarse de manera responsable y legal.
- **Buenas prácticas recomendadas**:

    - Combinar cookies y fingerprinting para un balance óptimo entre seguridad y experiencia de usuario.
    - En el caso de fingerprinting, informar claramente al usuario cuando se utilice, y aplicar técnicas como hash o cifrado de datos sensibles.
    - Adaptar dinámicamente las estrategias de seguimiento y tratamiento de datos en función de la jurisdicción del usuario, garantizando el cumplimiento normativo.

6. Medidas de Prevención contra el Web Tracking

El web tracking es una práctica extendida que permite a sitios web y a terceros rastrear y perfilar a los usuarios a través de distintas técnicas. Entre las más utilizadas se encuentran el tracking por cookies y el fingerprinting del navegador/dispositivo. En este apartado se exploran las estrategias y herramientas actuales para prevenir estas formas de seguimiento, enfocándonos en soluciones tanto a nivel de usuario como de arquitectura tecnológica.

6.1. Prevención del Tracking por Cookies

Las cookies son pequeños archivos almacenados en el navegador que contienen información sobre la actividad del usuario. El tracking por cookies, especialmente las cookies de **terceros (third-party cookies)**, permite crear perfiles detallados entre distintos sitios web.

6.1.1. Bloqueo de Cookies de Terceros

Navegadores como Firefox, Safari y Brave bloquean automáticamente las cookies de terceros. Chrome planea eliminarlas progresivamente mediante la iniciativa **Privacy Sandbox**, aunque con alternativas como el **Topics API** que siguen siendo discutidas por la comunidad.

Ventajas	Limitaciones
Fácil de aplicar.	Algunos sitios pueden romperse o restringir funcionalidad (ej. sistemas de login).
Protección inmediata contra la mayoría del tracking entre dominios.	No bloquea otros métodos como el fingerprinting.

6.1.2. Uso de Extensiones Antitracking

Más allá de las configuraciones internas del navegador, existen herramientas adicionales en forma de extensiones que bloquean el acceso a cookies utilizadas con fines de seguimiento. Extensiones como **uBlock Origin**, **Privacy Badger** o **Ghostery** son ampliamente reconocidas por su capacidad para detectar y bloquear scripts y dominios relacionados con el tracking.

Ventajas	Limitaciones
Análisis heurístico en tiempo real.	Puede requerir configuración adicional.
Personalización avanzada.	No bloquean todos los métodos emergentes de seguimiento.

6.1.3. Navegación en Modo Privado / Incógnito

Por otra parte, la navegación en modo privado o incógnito también proporciona cierto grado de protección, ya que las cookies generadas durante la sesión se eliminan al cerrarla. Sin embargo, esta medida es limitada, ya que las cookies siguen siendo funcionales durante el tiempo que dura la sesión, y no protege frente a técnicas más sofisticadas como el fingerprinting.

Ventajas	Limitaciones
Las cookies se eliminan al cerrar la sesión.	Las cookies de terceros se siguen utilizando durante la sesión.
Reduce la persistencia de seguimiento.	No bloquea fingerprinting ni otros identificadores pasivos.

6.2. Prevención del Fingerprinting

El fingerprinting consiste en recoger datos del navegador y dispositivo (fuentes, resolución, plugins, sistema operativo, idioma, etc.) para crear un identificador único, sin necesidad de almacenar nada localmente.

6.2.1. Uso de Navegadores con Protección Integrada

Debido a la naturaleza pasiva y no intrusiva del fingerprinting, su prevención resulta mucho más compleja. No obstante, algunos navegadores han desarrollado mecanismos

específicos para reducir su efectividad. El navegador **Tor**, por ejemplo, implementa una política estricta de uniformización de huellas digitales, haciendo que todos los usuarios parezcan iguales desde el punto de vista del fingerprinting. **Brave**, por su parte, emplea técnicas de aleatorización activa que modifican de forma controlada los parámetros del sistema para dificultar la reidentificación. **Firefox** también ha integrado funciones de protección contra fingerprinting dentro de su modo de protección mejorada contra rastreo, aunque su nivel de eficacia es algo inferior al de Tor o Brave.

Además, existen extensiones especializadas como ***CanvasBlocker*** que intervienen directamente en la ejecución de scripts relacionados con el fingerprinting, bloqueando el acceso a APIs como Canvas, WebGL o AudioContext, las cuales suelen ser utilizadas para obtener información gráfica y de hardware. Otras herramientas como ***NoScript*** o ***uMatrix*** ofrecen un control granular sobre los scripts que se ejecutan en cada página, impidiendo la recopilación no autorizada de datos.

Para usuarios con conocimientos técnicos avanzados, se pueden implementar estrategias más sofisticadas como la **virtualización del entorno de navegación**, **el uso de contenedores separados** o incluso **la navegación a través de máquinas virtuales**. Estas prácticas permiten segmentar completamente los contextos de uso y dificultar enormemente la correlación de datos entre sesiones o sitios web distintos.

7. Preguntas en la classe

1. **¿Qué técnica de web tracking os parece más “intrusiva”: cookies o fingerprinting? ¿Por qué?**

Solución:

- Fingerprinting, por su persistencia y porque no depende de almacenamiento local. Recordad que las cookies se pueden borrar, pero el fingerprinting sigue activo aunque limpiemos el historial.

2. **Teniendo en cuenta puedes aceptar o rechazar las cookies, en el caso del fingerprinting, muchos no somos conscientes de que está ahí, no sabemos qué tipo de información concreta recopila ni como la usa, que opináis de esto, tiene alguna ventaja o son todo desventajas?**

Solución:

- “Existe un marco legal que tienen que cumplir, como el RGPD, y usualmente si se utiliza fingerprinting para fines de seguimiento y perfilado, es necesario

obtener el consentimiento informado y explícito del usuario. ”

- “El usuario tiene derecho a acceder a sus datos y a solicitar su rectificación o supresión y se puede utilizar para detectar actividades fraudulentas, como la creación de múltiples cuentas falsas.

3. **¿Para qué se utilizan principalmente las cookies y el fingerprinting? ¿O creen que se pueden utilizar en otros contextos o con otros fines?**

Solución

- Las cookies y el fingerprinting se utilizan principalmente para rastrear la actividad del usuario en línea, personalizar la experiencia y mostrar publicidad dirigida. También pueden usarse en otros contextos, como seguridad (por ejemplo, detectar fraudes) o análisis de rendimiento de sitios web.

7. Bibliografia

https://www.avast.com/es-es/c-web-tracking

https://www.hotjar.com/es/seguimiento-web/

https://policies.google.com/technologies/cookies?hl=es

https://www.kaspersky.es/resource-center/definitions/cookies#:~:text=Es%20sencillo:%20el%20navegador%20web,datos%20de%20tus%20sesiones%20anteriores.

https://rockcontent.com/es/blog/cookies/#:~:text=Las%20cookies%20son%20archivos%20de,navegación%20en%20el%20sitio%20web.

https://www.hp.com/us-en/shop/tech-takes/what-are-computer-cookies#:~:text=Computer%20cookies%20are%20small%20files,the%20stored%20information%20about%20you.

https://www.exteriores.gob.es/es/Paginas/Cookies.aspx#:~:text=2.2.,unos%20minutos%20a%20varios%20años.

https://www.xataka.com/basics/que-cookies-que-tipos-hay-que-pasa-desactivas#:~:text=Las%20propias%20son%20las%20que,según%20la%20finalidad%20que%20tienen.

https://whyadsmedia.com/blog/que-son-las-cookies-en-internet-y-que-tipos-de-cookies-existen/

https://www.lisainstitute.com/blogs/blog/que-es-el-fingerprinting-huella-digital-de-nuestros-dispositivos#:~:text=de%20nuestros%20dispositivos-,¿Qué%20es%20el%20fingerprinting%20o%20huella%20digital%20y%20cómo%20se,Fraude%20del%20CEO

https://immune.institute/blog/que-es-fingerprinting-para-que-se-utiliza/

https://www.one.com/es/seguridad-de-su-web/que-es-la-huella-digital#:~:text=¿Cómo%20se%20obtienen%20las%20huellas,comportamiento%20y%20unas%20preferencias%20específicas.

https://ciberseguridad.com/amenzas/footprinting-fingerprinting/#:~:text=el%20sistema%20objetivo.-,¿Qué%20es%20Fingerprinting?,VPN%20o%20la%20red%20Tor.

https://bernanetwork.com/que-es-fingerprinting-ciberseguridad#:~:text=El%20fingerprinting%20es%20una%20técnica,instaladas%2C%20entre%20otros%20parámetros%20técnicos.

https://seon.io/es/recursos/glosario/canvas-fingerprinting/#:~:text=¿Cómo%20funciona%20el%20canvas%20fingerprinting,su%20software%2C%20actividad%20y%20características.

https://www3.cs.stonybrook.edu/~mikepo/papers/firstparty.www21.pdf

https://digitalcommons.morris.umn.edu/horizons/vol8/iss2/1/

https://developer.mozilla.org/en-US/docs/Web/Privacy/Guides/Third-party_cookies