How safe is the Metaverse?

PRIMERA ENTREGA

Amenazas a la seguridad y la privacidad del Metaverso

Las amenazas de seguridade típicas del Metaverso se pueden classificar a partir de las siguientes siete dimensiones: IDENTIDAD, DATOS, PRIVACIDAD, RED, ECONOMÍA, GOBIERNO y EFECTOS FÍSICOS/SOCIALES.

AMENAZAS RELACIONADAS CON LA IDENTIDAD

En el Metaverso, la gestión de la identidade desempeña un papel vital para los usuarios/avatares. Por ejemplo, los piratas informáticos pueden robar la información personal de los usuários a través de dispositivos personales pirateados, estafas de correo electrónico – phishing- y los datos de clientes robados de las empresas para cometer fraudes y delitos.

1. Ataque de suplantación

Un atacante puede llevar a cabo el ataque de suplantación haciéndose passar por otra entidad autorizada para aceder a um servicio o sistema del Metaverso.

Por ejemplo, los atacantes pueden explotar las amenazas de suplantación de Bluetooth para hacerse passar por puntos finales de confianza y aceder ilegalmente a los servicios del Metaverso insertando dispositivos falsos em el emparejamiento Bluetooth estabelecido.

Otro ejemplo es que los piratas informáticos pueden invadir headsets o dispositivos wearables y explotarlos como puntos de entrada para hacerse pasar por la víctima y obtener ilegalmente sus privilegios.

2. Vinculación de la identidad en los mundos ternarios

A medida que el Metaverso asimila la realidade em sí mismo, los mundos humano, físico y virtual se integran perfectamente em el Metaverso, provocando problemas de vinculación de identidad con los mundos ternários.

Ejemplo 1

Por ejemplo, un jugador malicioso A puede rastrear a otro jugador B e inferir su posición en el mundo real

Ejemplo 2

Los piratas informáticos pueden rastrear la posición de los usuários a través de auriculares o gafas de VR comprometidos

3. Autenticación fiable e interoperable

Para los usuarios/avatares em el Metaverso es fundamental garantizar uma identidade rápida, eficiente y de confianza entre plataformas y domínios de autenticación, es decir, a través de varios dominios de servicios y mundos virtuales.

AMENAZAS RELACIONADAS CON LOS DATOS

Los datos recogidos o generados por los usuarios, los dispositivos IoT y los avatares pueden sufrir amenazas em términos de confidencialidade, integridad, disponibilidade, inyección de datos falsos y rastreo del propietario/proveniência del Contenido Generado por los Usuarios (UGC) en el Metaverso

1. ATAQUE DE MANIPULACIÓN DE DATOS

Los adversarios pueden modificar, falsificar, substituir y eliminar los datos en bruto para interferir en las actividades normales de los usuarios, avatares o entidades físicas. Además los adversarios pueden pasar desapercebidos falsificando los archivos de regisro correspondientes o los resultados de la compilación de mensajes para ocultar sus rastros delictivos

2. ATAQUE DE INYECCIÓN DE DATOS FALSOS

Los atacantes pueden inyectar información falsificada, como mensajes falsos e instrucciones erróneas, para enganar a los sistemas metaversos. Por ejemplo, la creación de contenidos assistida por IA puede ayudar a mejorar la inmersión del usuário em la fase inicial del Metaverso, y los adversarios pueden inyectar muestras de entrenamiento adversas o gradientes envenenados durante el entrenamiento centralizado o distribuido de la IA, respectivamente, para generar modelos de IA sesgados.

1. AMENAZAS A LA CALIDAD DE LOS DATOS DEL UGC Y LA APORTACIÓN FÍSICA

En el Metaverso, los usuarios / avatares egoístas pueden contribuir a generar contenidos de baja calidad bajo la modalidad de UGC para ahorrar sus costes, lo que compromete la utilidad del UGC así como la calidad de los datos.

Por ejemplo, pueden compartir datos no alineados y severos durante el proceso entrenamiento colaborativo de la recomendación de contenidos e el Metaverso.

Otro ejemplo es que los sensores vestibles no calibrados pueden generar datos sensoriales inexactos e incluso erróneos para enganar la creación de gemelos digitales en el Metaverso

2. AMENAZAS A LA PROPIEDAD Y PROCEDENCIA DEL UGC

A diferencia del registro de activos supervisado por el Gobierno en el mundo real, el Metaverso es un espacio abierto y totalmente autónomo y no existe ninguna autoridade centralizada.

Debido a la falta de autoridad, es difícil rastrear la propiedad y la procedência de diversos UGC producidos por avatares masivos en diferentes mundos virtuales del Metaverso, así como convertir los UGC en activos protegidos.

AMENAZAS A LA PRIVACIDAD

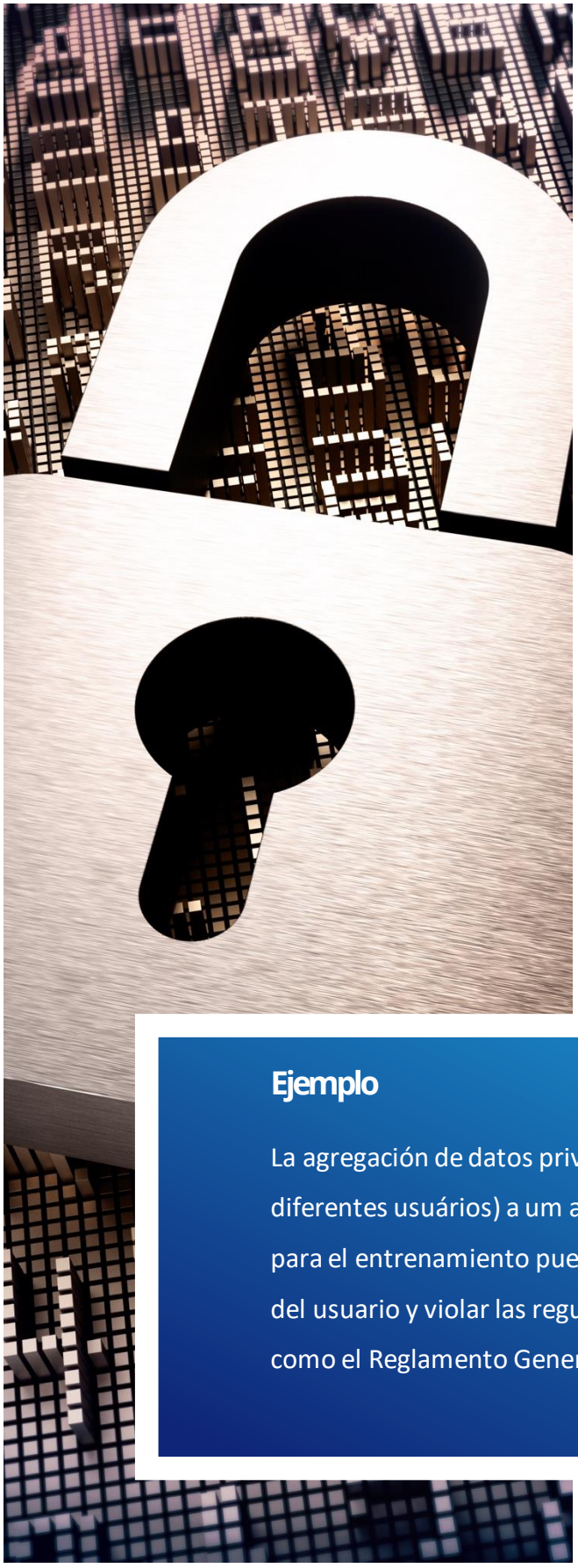
Cuando se disfruta de la vida digital en el Metaverso, la privacidad del usuario, incluida la privacidad de la ubicación, los hábitos, los estilos de vida, etc., puede verse ofendida durante el ciclo de vida de los servicios de datos, incluida la percepción, la transmisión, el procesamiento, la gobernanza y el almacenamiento de datos.

1. Recogida de datos generalizada

La construcción de un avatar requiere actividades omnipresentes de perfilado del usuário, incluyendo las expresiones faciales, los movimientos de los ojos y las manos, el habla y las características biométricas, los patrones de ondas cerebrales y el entorno. Por ejemplo, los sensores de movimento y las cuatro cámaras integradas en las Meta Quest 2 ayudan a rastrear la dirección y el movimiento de la cabeza, a dibujar nuestras habitaciones, así como a seguir nuestras posiciones y el entorno en tiempo real com precisión submilimétrica. Si es hackeado por atacantes, se pueden cometer graves delitos a partir de estos datos sensibles.

2. Fuga de privacidad en la transmisión de datos

En los sistemas metaversos, los datos massivos privados y sensibles de los usuários recogidos em varios dispositivos XR se transfieren a través de comunicaciones alámbricas e inalámbricas, cuya confidencialidade debe estar prohibida a indivíduos/servicios no autorizados. Aunque las comunicaciones estén cifradas y la información se transmita de forma confidencial, los adversarios pueden aceder a los datos sin processar espiando el canal específico e incluso rastrear la ubicación de los usuários mediante ataques diferenciales y ataques de inferencia avanzados.



3. Fuga de privacidad en el procesamiento de datos

En el Metaverso, la agregación y el procesamiento de datos massivos recogidos de cuerpos y entornos humanos son esenciales para la creación y la representación de avatares y metaversos, em los que puede filtrarse información sensible de los usuarios.

Ejemplo

La agregación de datos privados (pertenecientes a diferentes usuários) a um almacenamiento central para el entrenamiento puede ofender la privacidade del usuario y violar las regulaciones existentes, como el Reglamento General de Protección de Datos

4. Fuga de privacidad en el almacenamiento en la nube

El almacenamiento de esta información privada y sensible de usuarios masivos en servidores en la nube o dispositivos también puede plantear problemas de divulgación de la privacidade. Por ejemplo, los hackers pueden deducir la información de privacidad de los usuarios mediante consultas frecuentes a través de ataques diferenciales e incluso comprometer el almacenamiento em la nube mediante ataque DDoS.

5. Acceso no autorizado a datos

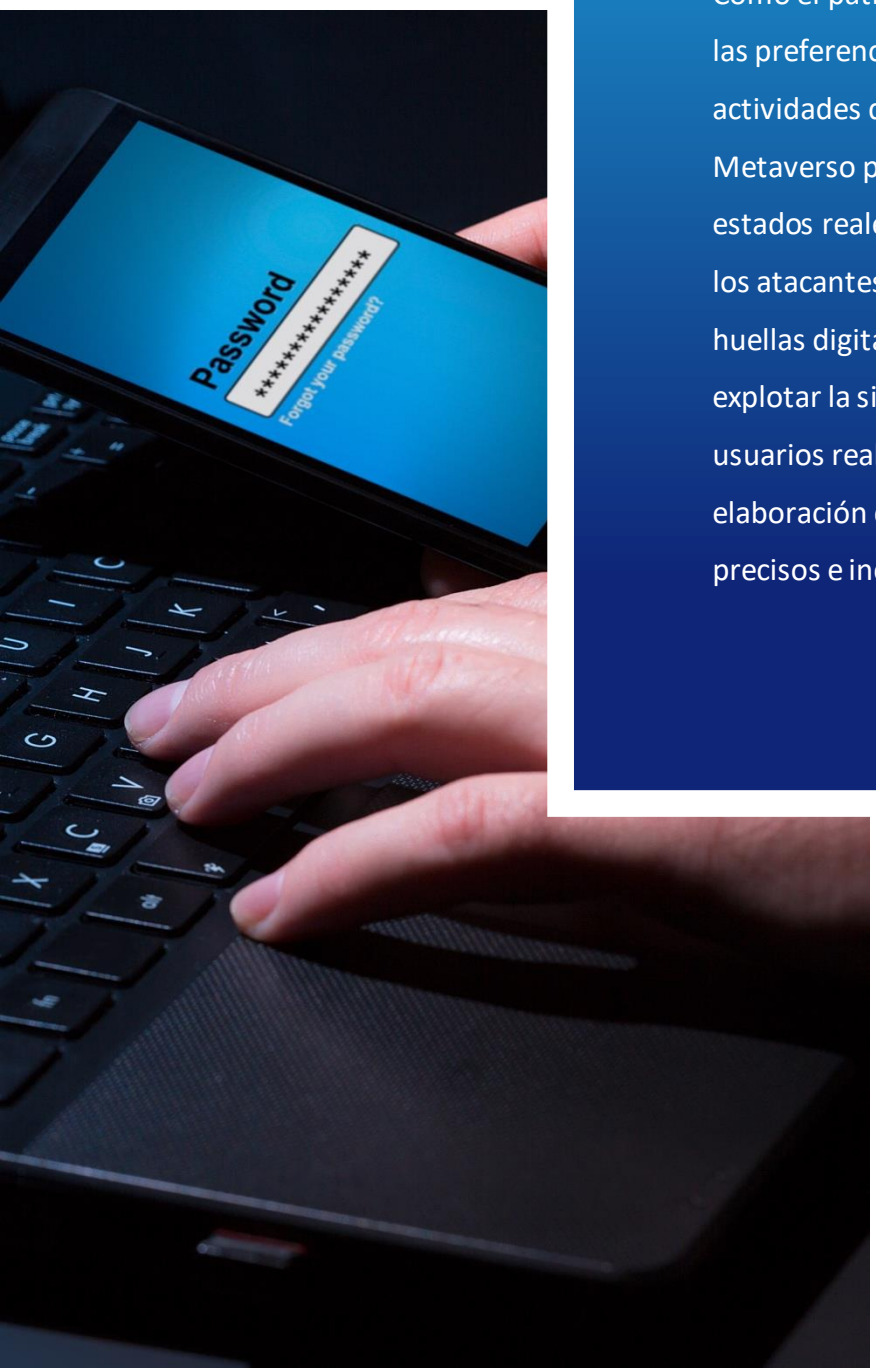
Para ofrecer servicios personalizados sin fisuras (por ejemplo, la apariencia personalizada del avatar) em el Metaverso, diferentes proveedores de servicios em distintos subversos necesitan aceder a las actividades de perfilado del usuario/avatar en tiempo real. Los proveedores de servicios malintencionados pueden elevar ilegalmente sus derechos de acceso a los datos mediante ataques como el desbordamiento del búfer y la manipulación de las listas de control de acceso.

6. Uso indebido de los datos del usuario/avatar

En el ciclo de la vida de los servicios de datos en el Metaverso, los datos relacionados com el usuario/avatar pueden ser revelados intencionadamente por los atacantes o involuntariamente por los proveedores de servicios para facilitar la elaboración de perfiles de usuario y actividades de marketing de precisión.

7. Amenazas a las huellas digitales

Como el patrón de comportamento, las preferencias, los hábitos y las actividades de los avatares en el Metaverso pueden reflejar los estados reales de su contraparte física, los atacantes pueden recopilar las huellas digitales de los avatares y explotar la similitud vinculada a los usuarios reales para facilitar la elaboración de perfiles de usuario precisos e incluso actividades ilegales.



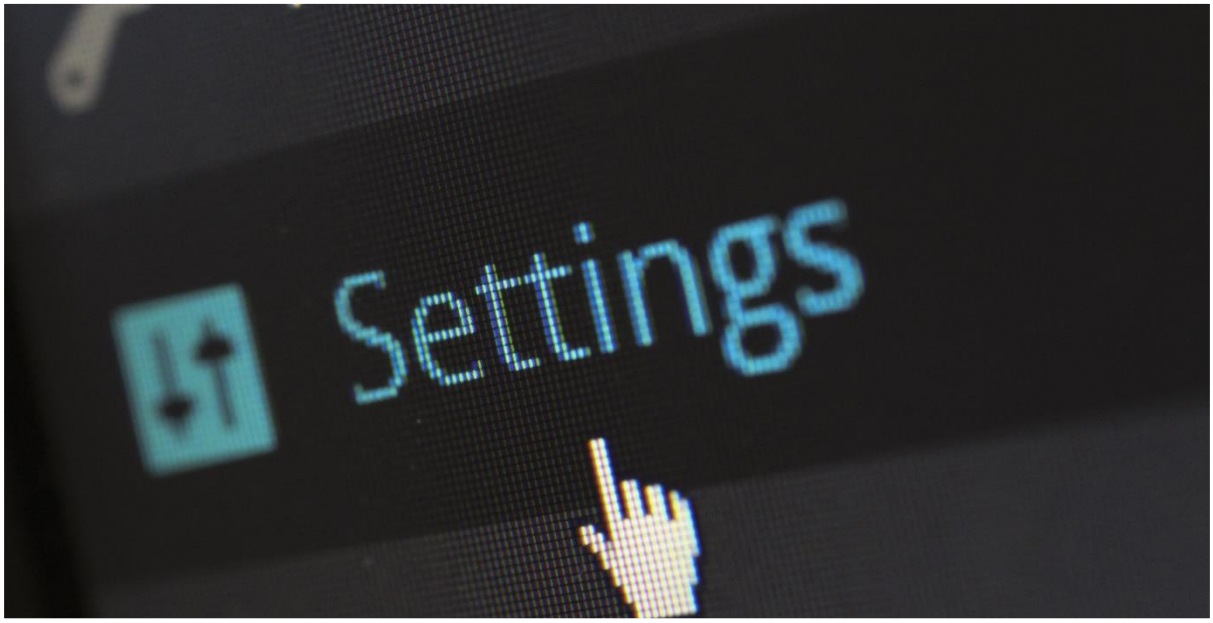
STEP 1

STEP 2

STEP 3

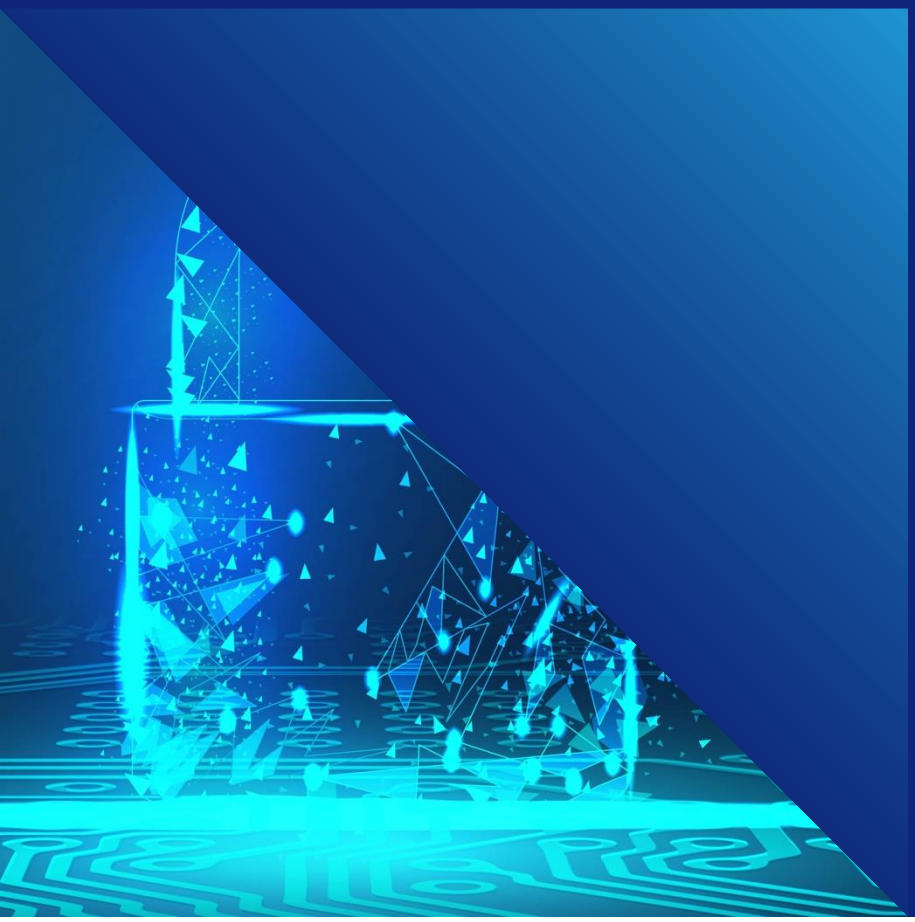
Además el Metaverso suele oferecer la vista en tercera persona com un ángulo de visión más amplio del entorno de su avatar que el del mundo real, lo que puede vulnerar la privacidad del comportamento de otros usuários sin que sean conscientes de ello.

Por ejemplo un avatar puede llevar a cabo el ataque de acoso/espionaje virtual siguiendo a su avatar y registrando todas sus huellas digitales, por ejemplo, los comportamientos de compra, para facilitar los ataques de ingeniería social.



8. Amenazas a la rendición de cuentas

Dado que los dispositivos XR recopilan intrinsecamente más datos sensibles, como la ubicación y el entorno de los usuarios, que los dispositivos inteligentes tradicionales, la rendición de cuentas en el Metaverso es importante para garantizar que los datos de los usuarios se manejen respetando la privacidad. Para los proveedores de servicios metaversos, el proceso de auditoria del cumplimiento de las normativas de privacidad (por ejemplo el Reglamento General de Protección de Datos) para la rendición de cuentas puede ser complicado y llevar mucho tempo bajo la arquitectura de oferta de servicios centralizada. Además, les resulta difícil garantizar la transparencia del cumplimiento de la normativa durante el ciclo de vida de la gestión de datos, especialmente en la nueva ecologia digital del metaverso.



PRIMERA ENTREGA

DE LA SERIE HOW SAFE IS THE METAVERSE?