Caso de éxito: implementación de autenticación biométrica en una empresa financiera

Integrantes:

Sebastian Montalvo Quiñones

Victor Paternina Suarez

1. ¿Por qué FinanSecure decidió realizar la comprobación de la huella o del rostro directamente en el teléfono en lugar de almacenar la información biométrica de todos los clientes en sus servidores? Argumenta las ventajas de esta decisión.

Porque la huella y la cara no se pueden cambiar. Si a uno le roban la contraseña la cambia y ya, pero si se filtra la huella no puede cambiar de dedo. Entonces si FinanSecure guardaba millones de huellas y rostros en un servidor, eso se volvía un botín demasiado grande para los atacantes. Haciendo la verificación en el mismo celular, el banco solo guarda la clave pública, que sola no le sirve a nadie, y aun así puede confirmar que el acceso viene del dispositivo autorizado. La ventaja es que se guarda únicamente lo que de verdad se necesita para prestar el servicio.

2. ¿Por qué el proceso de enrolamiento puede considerarse una de las etapas más importantes de un sistema de autenticación biométrica? Explica qué podría ocurrir si un atacante lograra registrar fraudulentamente su propio dispositivo.

Porque el enrolamiento es donde se decide qué teléfono queda amarrado a qué cliente. Si un atacante logra registrar su propio celular a nombre de otra persona, el sistema va a funcionar perfecto, pero protegiendo al delincuente, porque las firmas serían válidas y el servidor no vería nada raro. Por eso pusieron varios pasos antes de habilitarlo: entrar con las credenciales de siempre, el código enviado al número ya registrado y revisar que el dispositivo cumpliera ciertos requisitos de seguridad.

3. ¿Consideras que utilizar únicamente la huella digital o el reconocimiento facial sería suficiente para proteger todas las operaciones financieras de FinanSecure? Argumenta tu respuesta utilizando las medidas de seguridad descritas en el caso.

No, para nada. En la lectura queda claro que la seguridad dependía de varias cosas al tiempo: un enrolamiento seguro, la protección de las claves criptográficas, desafíos distintos en cada autenticación, comunicaciones cifradas, control de dispositivos, detección de comportamientos anormales, autenticación adicional en operaciones de alto riesgo y el registro y auditoría de los accesos. Una huella no es prueba absoluta de identidad, es apenas una parte del sistema.

4. Explica por qué el uso de un desafío diferente en cada inicio de sesión ayuda a proteger el sistema frente a ataques de repetición o replay. ¿Qué problema existiría si siempre se utilizara la misma información?

Porque cada vez que uno entra, el servidor manda un reto diferente y el teléfono lo firma con su clave privada, entonces esa firma sirve solo para ese momento. Si siempre se usara la misma información, un atacante que alcance a capturar el mensaje de una sesión vieja podría

reenviarlo después y el servidor lo aceptaría sin necesitar la huella ni el celular del cliente. Con el desafío cambiante, lo que capturó hoy mañana ya no le funciona.

5. En la apertura remota de cuentas, ¿por qué la comparación entre la selfie y la fotografía del documento no era suficiente? Argumenta la importancia que tuvo la incorporación de mecanismos de liveness.

Porque poniendo una simple foto delante de la cámara pasaba. El sistema veía una cara parecida a la del documento y daba el visto bueno sin saber si había una persona real ahí. Por eso metieron liveness, que analiza movimiento, profundidad, textura facial y cambios de iluminación, y en casos de mayor riesgo le pide al usuario girar la cabeza o seguir un punto en la pantalla. Igual el liveness no es perfecto, puede dejar pasar un ataque o rechazar a una persona legítima, y por eso los casos dudosos pasaban a revisión humana.

6. ¿Por qué FinanSecure mantuvo métodos alternativos de autenticación, aunque la implementación biométrica hubiera tenido buenos resultados? Argumenta tu respuesta considerando accesibilidad, fallos tecnológicos y pérdida de dispositivos.

Porque no todo el mundo puede usarla. Había clientes con teléfonos viejos sin sensores adecuados, otros a los que no les leía bien la huella y otros que simplemente no querían usar biometría. Si eso fuera lo único, esas personas quedaban por fuera del servicio. Y sumémosle los fallos técnicos y la pérdida del celular. Entonces mantener otra opción es tema de accesibilidad y también de que el cliente no se quede sin poder entrar a su cuenta.

7. Si un cliente pierde su teléfono, ¿por qué resulta importante que FinanSecure pueda revocar la clave asociada al dispositivo? Explica cómo este mecanismo permite recuperar la seguridad sin necesidad de cambiar las características biométricas de la persona.

Porque con solo borrar la clave pública de ese teléfono, todas las firmas hechas con la clave privada dejan de ser aceptadas por el servidor. Ahí ese celular queda inservible para entrar a la cuenta, así el ladrón lo tenga en la mano. Y cuando el cliente compra otro, repite el proceso seguro de enrolamiento y listo. Esa es la ventaja frente para guardar biometría en el servidor: uno revoca la credencial y emite una nueva sin tener que tocarle la huella ni el rostro a la persona, que eso sí no se puede volver a emitir.

8. A partir del caso, argumenta si el éxito de FinanSecure se debe principalmente a utilizar biometría o al diseño completo de su sistema de autenticación. Sustenta tu posición mencionando al menos cuatro controles o decisiones de seguridad descritos en la lectura.

Nosotros creemos que fue el diseño completo. La biometría fue la parte visible y la que mejoró la experiencia del usuario, pero lo que sostuvo la seguridad fue todo lo que estaba alrededor. Mencionamos cuatro: el enrolamiento con varias comprobaciones, que evita que un atacante registre su propio celular; las claves criptográficas con la privada guardada dentro del dispositivo, así el banco nunca recibe huellas ni rostros; el desafío distinto en cada autenticación, que tumba los ataques de repetición y le quita sentido al phishing porque no hay una credencial reutilizable que robar; y la autenticación adicional según el riesgo, que pide un

segundo factor cuando aparece un dispositivo nuevo, una ubicación rara o una transferencia de gran valor.

Además de eso estaba el liveness en la apertura de cuentas, la revocación de claves cuando se pierde el teléfono, la auditoría de los accesos y los métodos alternativos. Como dice la conclusión del caso, la biometría puede aumentar la seguridad, pero su valor real depende de cómo se integre dentro de todo el sistema de autenticación.