Seguridad en los sistemas biométricos

Presentación

El objetivo de esta PEC es el análisis desde el punto de vista de la seguridad de un sistema real. Esta PEC está compuesta por un único ejercicio con varios apartados.

Competencias

Conocer los puntos débiles de los sistemas biométricos en lo que respecta a su seguridad.

Objetivos

Evaluar la idoneidad de los sistemas biométricos en función del contexto.

Conocer los posibles ataques de un sistema biométrico específico y los mecanismos para proteger el sistema y hacerlo más seguro.

Descripción de la práctica

En la Universidad Rovira i Virgili, están preparando un congreso internacional y nos han pedido ayuda respecto a la seguridad del sistema de recogida de credenciales y entrada a las distintas salas. Después de pasearnos por las distintas áreas del congreso y hablar con los organizadores, pasamos a detallar el sistema utilizado.

La matriculación de los asistentes al congreso lo lleva a cabo personal autorizado en unas dependencias de la propia Universidad. Allí es donde los asistentes se tienen que identificar mostrando el pasaporte. Después de comprobar que el asistente ha pagado la inscripción al congreso, se registra la huella dactilar de uno de sus dedos y se toma una fotografía de la cara. Tanto la huella como la fotografía se envía a un ordenador que extrae las características de la huella dactilar y almacena en una base de datos remota dichas características, junto con la fotografía de la cara y el nombre del usuario. Dicha base de datos se encuentra en los ordenadores centrales de la universidad, en otro edificio y el servicio de informática es el encargado de su mantenimiento.

En las entradas de las salas de conferencias hay personal autorizado que realiza la identificación de los asistentes con ordenadores portátiles. Estos llevan incorporados un sensor Futronic de huella dactilar en el mismo teclado y están conectados a Internet a través de la red WiFi de la Universidad. En estos portátiles está instalada la aplicación que captura la huella dactilar. Dicha aplicación recibe la imagen de la huella dactilar creada por el sensor biométrico, extrae las características de la huella y las envía a la base de datos remota. En el ordenador central de la Universidad una aplicación busca en la base de datos la huella dactilar capturada por el sensor y devuelve la información del usuario que ha generado la menor

distancia entre huellas dactilares. En el caso que la mínima distancia sea mayor que el umbral **A**, entonces devuelve “no encontrado”. Cuando los portátiles reciben la información, muestran por pantalla la fotografía de la cara de la persona identificada, así como el nombre del usuario. Obviamente, si la base de datos devuelve “no encontrado”, entonces el portátil muestra por pantalla este mensaje. Según la imagen que aparece en pantalla, el personal autorizado toma la decisión de dejar pasar al congresista o no.

A partir de la información que os hemos proporcionado de este sistema biométrico contestad a las siguientes preguntas respecto **a la fase de identificación** de los asistentes al congreso:

a) Identificad y detallad qué partes de los procesos detallados corresponde a cada uno de los nueve puntos que aparecen en la figura 1 de la página 11 del módulo “Seguridad en los sistemas biométricos”.

b) Explicad sí es posible que se puedan realizar los siguientes ataques y en qué puntos se pueden producir.

   1) Ataque de biometría falsa.

   2) Inyección de paquetes falsos.

c) Dados los ataques comentados en la sección anterior, explicad cómo creéis que se podría fortalecer la seguridad del sistema.

d) Comentad cómo influye el umbral **A, tanto si es muy alto como muy bajo,** en el proceso de identificación de los asistentes al congreso y qué decisión tomarías al respecto.

Recursos

- Documentación de los módulos:
  - La biometría para la identificación de las personas (módulo 1).
  - Seguridad en los sistemas biométricos (módulo 6).

Criterios de evaluación

Todas las cuatro preguntas tienen el mismo peso

Recordad que según el plan docente:

Nota Final = 25% PEC1 + 30% PEC2 + 30% PEC3+ 15% PEC4

Formato y fecha de entrega

El documento que tenéis que adjuntar tiene que estar en formato PDF. No se aceptará ninguna solución que NO esté en este formato.

La fecha de entrega es el 26 de mayo de 2020.

Nota: **Propiedad intelectual**

A menudo es inevitable, al producir una obra multimedia, hacer uso de recursos creados por terceras personas. Es por tanto comprensible hacerlo en el marco de una práctica de los estudios del Grado de Multimedia, siempre que esto se documente claramente y no suponga plagio en la práctica.

Por lo tanto, al presentar una práctica que haga uso de recursos ajenos, se presentará junto con ella un documento en el que se detallen todos ellos, especificando el nombre de cada recurso, su autor, el lugar donde se obtuvo y el su estatus legal: si la obra está protegida por copyright o se acoge a alguna otra licencia de uso (Creative Commons, licencia GNU, GPL ...). El estudiante deberá asegurarse de que la licencia que sea no impide específicamente su uso en el marco de la práctica. En caso de no encontrar la información correspondiente deberá asumir que la obra está protegida por copyright.

Deberán, además, adjuntar los archivos originales cuando las obras utilizadas sean digitales, y su código fuente si corresponde.
Otro punto para considerar es que cualquier práctica que haga uso de recursos protegidos por copyright no podrá en ningún caso publicarse en *Mosaic*, la revista del Grado de Multimedia en la UOC, a no ser que los propietarios de los derechos intelectuales den su autorización explícita.