JNIC - Programa de Transferencia

Ficha de reto científico

Edición 2017

1 FICHA DE RETO

El mero hecho de proponer un reto a través del presente formulario implica la aceptación de las bases del Programa de Transferencia JNIC.

El formulario o Ficha Reto para documentar la propuesta de reto contiene los siguientes campos.

FICHA DE RETO JNIC

A. INFORMACIÓN SOBRE LA EDICIÓN DEL PROGRAMA EN LA QUE SE PRESENTA EL RETO

A.1 Edición Programa Transferencia JNIC: **2017**

B. INFORMACIÓN SOBRE EL RETADOR

B.1 Nombre de la Organización: ElevenPaths. Telefónica cyber security unit.

B.2 Portal web: (de la organización o aquel en el que haya información sobre el reto propuesto)
www.elevenpaths.com

B.3 Persona de contacto: Nombre, cargo, email, teléfono contacto.
Marcos Arjona, Consultor de Investigación e Innovación, marcos.arjona@11paths.com, 666985706.

B.4 Información de soporte (buzón de email / teléfono u otros) para dar respuesta a las dudas que los investigadores puedan plantear sobre el reto:
marcos.arjona@11paths.com

C. CARACTERÍSTICAS RELATIVAS AL RETO

C.1 Tipo de reto (abierto / restringido): Restringido

C.2 Se facilitará información confidencial que requiera un acuerdo previo formal (SI/NO): SI

C.3 Tipo de incentivo:

Nota: Es objetivo del Programa la publicación de los resultados obtenidos fruto de la investigación realizada para la solución del reto.

- ☐ Sin incentivos
- ☐ Premio en metálico mejor/es propuesta/s
- ☐ Financiación de la investigación para generación de prototipo o una PoC
- ☒ Reconocimiento para la mejor/es propuesta/s
- ☒ Utilización de instalaciones/equipos del retador durante la investigación
- ☒ Otros

Comentarios sobre los incentivos seleccionados:
ElevenPaths realizará un esfuerzo de difusión en sus medios de comunicación, así como en eventos y jornadas de índole científica donde se podrán presentar conjuntamente con el equipo de investigación, los avances actuales y el progreso de la solución al reto. Además, ElevenPaths apoyará en todo momento la hoja de ruta, facilitando el uso de las instalaciones, sistemas y datos necesarios para cumplir con los objetivos de la solución.

El vínculo entre la entidad investigadora junto a ElevenPaths podrá generar un proceso colaborativo propicio para ambas instituciones, mejorando el clima de cooperación y facilitando investigaciones y desarrollos relacionados con el reto en curso.
Los equipos investigadores que trasladen el conocimiento y producción de los retos a iniciativas empresariales propias o spin-offs podrán optar de manera privilegiada al programa de emprendimiento y aceleración de Wayra, una iniciativa de Telefónica a través de Open Future que se facilitará a las empresas siempre que cumplan con las características de admisión necesarias.
Pese a no tener un fondo de financiación definido, ElevenPaths realizará un seguimiento proactivo de la solución al reto, agilizando e incentivando su desarrollo, fomentando nuevas colaboraciones en el ámbito de la solución. Finalmente, según el progreso del reto podrían establecerse contratos privados de investigación sobre el reto para la creación del PoC o su continuidad.

C.4 (si procede) Cuantía económica para el premio a la mejor propuesta
Haga clic aquí para escribir texto.

C.5 (si procede) Cuantía económica para la financiación (1 año de trabajo investigador).
Haga clic aquí para escribir texto.

C.6 Se solicita revisión previa de cualquier publicación científica generada en la resolución del reto (SI/NO):
SI

C.7 Servicios que se ponen a disposición (utilización de hardware/software, posibilidad de estancias en las instalaciones del retador para conocer el reto, etc.):
Licencias de uso de plataformas de ElevenPaths.
Acceso a las plataformas pertinentes.

C.8 Requisitos de confidencialidad (tanto para los investigadores, como para los miembros del Comité que evalúen la propuesta):
Acuerdo de Confidencialidad sobre la documentación y software utilizado por los investigadores durante la ejecución del reto.

C.9 Condiciones de aceptación (limitaciones para la aceptación de solicitudes):
- Posesión de experiencia en el ámbito del reto bien sea a través de publicaciones en conferencias o revistas.
- Se valorará positivamente desarrollos previos y PoC realizados por el mismo equipo científico en áreas científicas similares o cuyo conocimiento pueda proporcionar valor añadido a la solución.

C.10 Condiciones de rechazo (cuestiones que quieran evitarse en las solicitudes):
- Equipo de investigación no consolidado o sin trayectoria científica demostrable.
- Solución no orientada a la posible comercialización del producto bien por restricciones funcionales o tecnológicas.

D. RETO PROPUESTO

D.1 Título del reto:
Autenticación continua e identificación adaptativa en dispositivos móviles.

D.2 Antecedentes:
Los mecanismos de identificación y control de acceso han adquirido una importancia crucial a la hora de habilitar o impedir el acceso a los dispositivos y a las aplicaciones. En concreto, una adecuada autenticación de los usuarios permite gestionar los privilegios y derechos de uso de SmartPhones. Evitando un uso indebido de los mismos sin autorización del propietario. Pero a su vez gracias a la constante validación de la identidad del usuario se puede facilitar la gestión de elementos de seguridad, permitiendo incluso que los usuarios

no tengan que depender constantemente del uso de contraseñas, pines o factores adicionales de autenticación. Dicho proceso de autenticación continua permite un enfoque holístico, permitiendo su aplicación tanto a entornos domésticos como a empresariales.

D.3 Motivación:

ElevenPaths y Telefónica poseen un amplio catálogo de productos y servicios cuyo primer elemento de seguridad radica en los distintos mecanismos de autenticación e identificación embebidos. Dichos elementos prestan una labor fundamental a la hora de identificar y gestionar el control de acceso a los dispositivos. Por tanto, uno de los objetivos de ElevenPaths consiste en realizar un constante esfuerzo para examinar nuevos enfoques y propuestas a dichos procesos de autenticación. Evaluando aquellas soluciones innovadoras que aporten un valor diferencial, garantizando capacidades no comunes de identificación y autenticación del usuario y aliviando las constantes medidas de verificación del usuario. Permitiendo una mejor experiencia de usuario sin provocar perjuicio alguno a su estado integral de seguridad y a su percepción de las medidas activas de protección.

D.4 Descripción del reto:

Esta propuesta plantea al equipo de investigación el diseño de un mecanismo de identificación y autenticación continua de usuarios, realizando un análisis de manera desapercibida durante el uso cotidiano de dispositivos móviles, tales como SmartPhones o Tablets. Debido a la gran variedad de recursos tecnológicos, de comportamiento y biométricos se valorarán aquellas propuestas que realmente puedan proporcionar una solución práctica y usable, no intrusiva y que no requiera de una elevación de privilegios en el dispositivo, algo que resultaría inviable de cara a la comercialización.

Entre los distintos enfoques, el equipo de investigación tiene cierta libertad para elaborar su propuesta de solución. Por tanto, cualquier combinación de sensores, gestos, comportamientos y muestras biométricas serán admitidas siempre que pueden abordar de manera realista el reto. Entre dichas opciones disponibles podemos encontrar:

- Uso de los sensores: giroscopio, de proximidad, giroscopio, podómetro, etc.
- Gestos y recorridos en la pantalla.
- Pulsaciones y comportamiento en la pulsación.
- Gestos en el patrón de la pantalla de inicio.
- Análisis de audio y vídeo.
- Movilidad con el dispositivo bloqueado.
- Otros

El objetivo principal es permitir la identificación y autenticación de los usuarios de manera alternativa, mejorando la seguridad gracias a distintos mecanismos de reconocimiento o análisis que no pueden ser falseados de manera trivial.

D.5 Recursos de apoyo que se pondrán a disposición de los investigadores (data-sets, etc.):

Según la solución, alcance y tipo de enfoque se proporcionará al equipo de investigación acceso a la información, conjuntos de datos y APIs necesarias para la resolución del reto. Esta cesión documental puede estar sujeta a un acuerdo de confidencialidad debido a su naturaleza privada y corporativa.

D.6 Avances realizados actualmente por el retador:

ElevenPaths ha realizado una prospección de las distintas metodologías, técnicas y herramientas existentes. Evaluando el estado del arte actual en cuanto a tecnologías de identificación y autenticación continua, contextual, dinámica e implícita. De todas ellas es posible aprovechar los mecanismos en mayor o menor medida, pero no se ha realizado ninguna prueba de concepto sobre las posibilidades reales en entornos domésticos ni corporativos.

D.7 Alcance:

Prueba de Concepto usable con un TRL 5 que permita la autenticación de usuarios correctamente con un reducido margen de duda. Entre los objetivos buscados existirán ciertos indicadores de éxito funcionales para identificar el alcance como son:

- Prevenir o esquivar los mecanismos de seguridad que impiden la captura de datos del usuario en determinados estados, como ocurre con el dispositivo bloqueado.
- Capacidad para ignorar el doble factor de autenticación gracias a la identificación inequívoca de los usuarios.
- Capacidad de bloquear el dispositivo si el comportamiento no coincide con es habitual del usuario.
- Monitorización y trazado de distintas identidades de usuarios.
- Técnicas para identificar usuarios con o sin entrenamiento
- Dashboard para visualizar datos como la precisión en la identificación de usuarios y distintas acciones facilitadas al usuario gracias a la autenticación continua.
- Soporte para varios usuarios autorizados
- Integración con otras tecnologías móviles de ElevenPaths.
- Diseño modularizado permitiendo la incorporación de futuras mejoras, extensiones y funcionalidades de respuesta y control de dispositivos ante anomalías. (Captura de imágenes, monitorización de redes conectadas, registro de datos accedidos, gestión remota, etc.)

D.8 Casos de uso:

CU1:

Precondición: Alice es una empleada que posee privilegios de acceso y uso de una serie de datos bancarios de la empresa a través de la tablet corporativa. Por distintos motivos Alice deja olvidada en la sala de reuniones dicha tablet, correctamente bloqueada. Pero aún así, existen una serie de riesgos de seguridad asociados a que otros individuos no autorizados accedan a dichos datos. Dicha Tablet está pareada con los auriculares bluetooth de Alice, e incluso tiene habilitada la opción de que si ambos dispositivos se encuentran próximos entre sí, la tablet se desbloquea automáticamente.

Descripción: Bob es un empleado descontento y encuentra la Tablet de Alice. Además, sabe que Alice siempre lleva consigo los auriculares bluetooth en uso ya que es un elemento imprescindible para el desempleo de su trabajo. Por tanto, Bob se acerca a Alice con cualquier excusa y de manera desapercibida Bob consigue desbloquear la tablet. Esto permite un acceso completo e identificado al contenido del dispositivo. Inmediatamente Bob se dispone a localizar la información bancaria, cuya intención radica en conocer la información salarial de sus compañeros.

Secuencia:

1) Bob recorre el repositorio a la búsqueda de hojas de cálculo con nombres que indiquen algo relativo a los salarios y la contabilidad.
2) Durante su búsqueda abre y cierra archivos para comprobar su contenido
3) Bob prueba a hacer búsquedas en los nombres de los ficheros del repositorio, encuentra uno que podría coincidir con el que esperaba encontrar.
4) Al intentar abrir este fichero, el sistema bloquea el dispositivo y éste internamente notifica una anomalía de autenticación del usuario activo.
5) Bob abandona el dispositivo y no consigue acceder a la información esperada.

Postcondición:

Los archivos privados no han sido comprometidos y el riesgo de seguridad ha sido mitigado y además las capacidades reactivas integradas como tracking, captura de imágenes por la cámara, localización y monitorización pueden aportar más datos e incluso identificar quién ha podido usar el dispositivo.

CU2:

Precondición: Carlos posee un dispositivo móvil con una normativa muy restringida de seguridad debido a los elevados privilegios que dispone a nivel corporativo para acceder y gestionar distintos recursos de la empresa. Dicho dispositivo no almacena credenciales ni contraseñas ni ningún tipo de token de seguridad que pudiera usar un tercero.
Descripción: Este usuario ve lastrada su actividad habitual por el elevado número de ocasiones en las que tiene que introducir su contraseña y patrones de desbloqueo. Incluyendo las repeticiones donde las ha introducido incorrectamente. El nuevo sistema de autenticación continua se incorpora a su dispositivo donde permanece residente y en modo entrenamiento durante un mes. La intención es aliviar su interacción con los mecanismos de seguridad de alguna manera.
Secuencia:

1) Carlos comienza su navegación por el interfaz web de la empresa y se autentica manualmente en el panel de entrada de la plataforma.
2) Durante su operación, requiere la conexión con un módulo externo que solicita otras credenciales. Por lo cual abre el panel de login de dicho módulo
3) Durante el uso del dispositivo, el sistema de autenticación continua entrenado ha conseguido identifica a Carlos con una probabilidad del 98% y por tanto automáticamente autoriza la solicitud de logeo y acceso al módulo externo
4) Este proceso es independiente de cualquier otra autenticación previa de Carlos, por lo que se realiza de manera individual en cada operación de login.
5) Carlos no recibe la solicitud de credenciales y puede acceder al módulo externo sin ningún inconveniente

Postcondición: El sistema de autenticación continua ha permitido trasladar la identidad del usuario al módulo externo, de manera inequívoca. Por tanto el usuario accede correctamente identificado y autenticado, de la misma forma que un usuario que hubiese introducido sus credenciales, pero con el respaldo de seguridad de ser un mecanismo continuo infalsificable.

D.9 Soluciones actuales que dan cobertura parcial al reto:

https://www.keytrac.net/
https://typingdna.com/
https://www.behaviosec.com/

D.10 Estudios/Investigaciones relacionados:

Banerjee, S. and Woodard, D. (2012) “Biometric Authentication and Identification Using Keystroke Dynamics: A Survey”. Journal of Pattern Recognition Research, 7, 116-139. (PDF)

Khan H., Atwater A., Hengartner U. (2014) “A Comparative Evaluation of Implicit Authentication Schemes”. In: Stavrou A., Bos H., Portokalidis G. (eds) Research in Attacks, Intrusions and Defenses. RAID 2014. Lecture Notes in Computer Science, vol 8688. Springer, Cham (PDF)

Pin Shen Teh, Ning Zhang, Andrew Beng Jin Teoh, and Ke Chen. 2016. A survey on touch dynamics authentication in mobile devices. Comput. Secur. 59, C (June 2016), 210-235. (PDF)

Mario Frank, Ralf Biedert, Eugene Ma, Ivan Martinovic, and Dawn Song. 2013. Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication. Trans. Info. For. Sec. 8, 1 (January 2013), 136-148 (PDF)

D.11 Documentación/Bibliografía de interés:

Gascon, Hugo et al. “Continuous Authentication on Mobile Devices by Analysis of Typing Motion Behavior.” Sicherheit (2014). (PDF)

P. Chairunnanda, N. Pham and U. Hengartner, "Privacy: Gone with the Typing! Identifying Web Users by Their Typing Patterns," 2011 IEEE Third International Conference on

Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing, Boston (PDF)
Gascon, Hugo et al. "Continuous Authentication on Mobile Devices by Analysis of Typing Motion Behavior." Sicherheit (2014). (PDF)

D.12 Otras consideraciones a tener en cuenta:
Los equipos de investigación que aborden estas soluciones no deben limitar su enfoque científico ni acotar su ambición tecnológica a los términos expresados en este reto si esto supone un perjuicio de cara a la ambición o a las expectativas alcanzables por los investigadores. Se valorará positivamente la incorporación de factores de valor diferenciales que permitan trazar una hoja de ruta mucho más ambiciosa, innovadora y comercializable.

E. SEGUIMIENTO

E.1 Hitos esperados (puntos de seguimiento de la investigación):
La lista de milestones serán factores que se acordarán adecuadamente con los equipos de investigación implicados, de esta manera se podrán adaptar las expectativas a criterios reales tales como la experiencia de los investigadores y el tipo de solución propuesta. Sin embargo, sigue siendo deseable obtener dos hitos clave:

1) Análisis de la viabilidad tecnológica del proyecto y la solución descrita.
2) PoC con TRL 5 que permita la identificación de usuarios de manera correcta

E.2 **TRL** objetivo para el primer año (Nivel de madurez que se espera que tengan las propuestas de solución recibidas): TRL2

F. EVOLUCIÓN DEL RETO

F.1 **TRL** objetivo para el final de la investigación (Nivel de madurez final que desea el retador para dar por finalizado el reto de forma exitosa):
TRL5

F.2 **Plazo** del reto (fecha límite para alcanzar el TRL final de investigación):
18 meses

http://2017.jnic.es/