

Desarrollo seguro de aplicaciones móviles

Introducción

Unidad 5

Contenidos

- 1 Principios básicos de seguridad en el desarrollo
 - El ciclo de desarrollo de software seguro
 - El S-SDLC en entornos ágiles
- 2 Buenas prácticas en el desarrollo seguro
- 3 Buenas prácticas en el desarrollo móvil
 - Protección de la aplicación
 - Manejo de datos sensibles
 - Logs* y filtrado de información sensible
 - Componentes HTML en aplicaciones móviles
 - Comunicación entre aplicaciones
 - Autenticación en aplicaciones móviles
- 4 Laboratorio
 - Android
 - iOS
- 5 Ejercicios de investigación
 - Test de evaluación



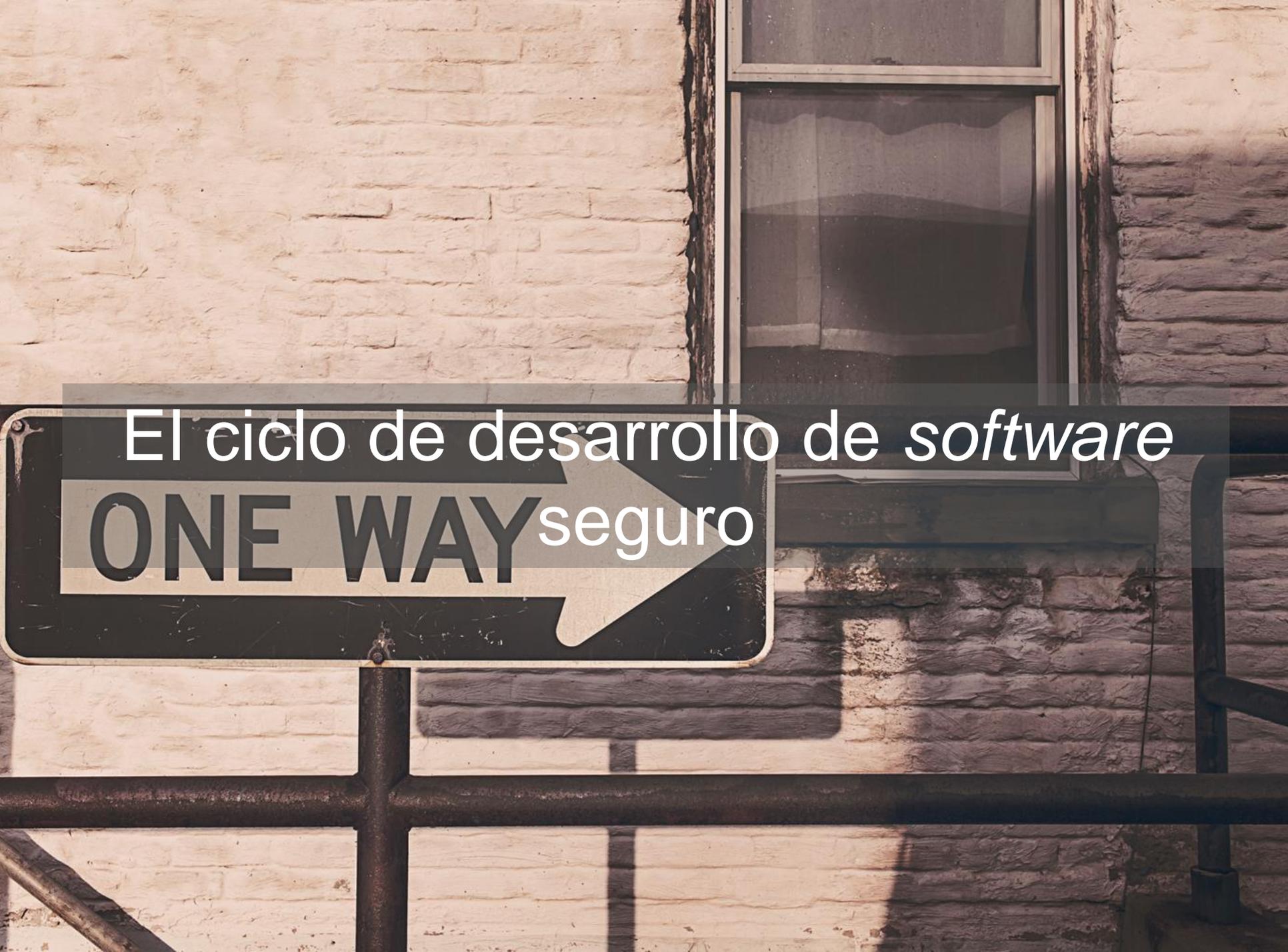


Principios básicos de seguridad en el desarrollo

◆◆◇ Principios de seguridad en el desarrollo

Introducción

- Las vulnerabilidades y problemas de seguridad pueden afectar a un producto *software* durante todo su desarrollo:
 - No identificando requisitos de seguridad durante la fase de análisis.
 - Creando diseños con fallos de seguridad.
 - Generando vulnerabilidades durante la etapa de implementación.
 - Desplegando el *software* de forma inadecuada.
 - No respondiendo de forma oportuna a los incidentes de seguridad que ocurran.
- Estos problemas, afectan directamente al *software* que se ha desarrollado y la información almacenada, pero también pueden afectar a:
 - Otras aplicaciones que se ejecutan en el entorno compartido.
 - El sistema del usuario (incluidos los dispositivos móviles).
 - Otros sistemas que interaccionan con el *software* a desarrollar.

A photograph of a brick wall with a window. A black 'ONE WAY' street sign with a white arrow pointing right is mounted on a metal post. The sign is overlaid with a semi-transparent dark grey box containing white text. The text reads 'El ciclo de desarrollo de software' in a serif font, 'ONE WAY' in a bold sans-serif font, and 'seguro' in a serif font.

El ciclo de desarrollo de *software*
ONE WAY seguro

◆◆◇ El ciclo de desarrollo de *software* seguro

Introducción

- El Ciclo de Desarrollo de *Software* Seguro o *Secure Software Development Life Cycle* (de aquí en adelante lo llamaremos **S-SDLC** por sus siglas en inglés) es un proceso de desarrollo de *software* que incorpora la seguridad como un elemento transversal durante todo el proceso de desarrollo.
- La incorporación de la seguridad como un elemento transversal del desarrollo de *software* se denomina “*Security By Design*”.
- La mayoría de vulnerabilidades **pueden solucionarse en la fase de desarrollo** de las aplicaciones, ya que muchas de ellas se crean dependiendo de como se implementen los procesos de desarrollo y sus controles asociados.
- El S-SDLC tiene en cuenta desde el inicio del desarrollo de *software*, todos los aspectos de seguridad que puedan estar involucrados en el mismo:
 - Permite detectar vulnerabilidades durante etapas tempranas en el desarrollo.
 - Ahorro de costes en vulnerabilidades detectadas en sistemas en producción.
 - Permite tener en cuenta los requisitos de conformidad a distintas regulaciones y estándares desde el principio del desarrollo.
 - Ahorro de costes para la incorporación de nuevos requisitos o funcionalidades destinadas a la conformidad.

◆◆◇ El ciclo de desarrollo de *software* seguro

Aproximaciones al S-SDLC

- Existen diferentes aproximaciones al S-SDLC:
 - OWASP CLASP (Comprehensive, Lightweight Application Security Process):
 - https://www.owasp.org/index.php/Category:OWASP_CLASP_Project
 - Microsoft Secure Development Lifecycle:
 - Desarrollada por Microsoft pero aplicable a cualquier desarrollo.
 - <https://www.microsoft.com/en-us/sdl/>
 - Digital's Security Touchpoints:
 - Desarrollados por Gary McGraw.
 - <http://www.swsec.com/resources/touchpoints/>
 - NIST 800-64:
 - Conjunto de consideraciones de seguridad a tener en cuenta durante el SDLC propuestas por el NIST.
 - <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-64r2.pdf>
- En general, todos los modelos incorporan una serie de actividades de seguridad al ciclo de vida del desarrollo.

◆◆◆ El ciclo de desarrollo de *software* seguro

Fases



◆◆◇ El ciclo de desarrollo de *software* seguro

Formación

- No es estrictamente una fase del S-SDLC pero es indispensable para poder llevarlo a cabo.
- El personal técnico que participe en el desarrollo debe ser capaz de llevar a cabo todas las tareas adicionales que se requieran para ser capaz de llevar a cabo el S-SDLC.
- Los conceptos que deben conocer incluyen:
 - Arquitecturas seguras.
 - Modelado de amenazas.
 - Codificación segura.
 - *Penetration testing*.
 - Prácticas de seguridad y privacidad.
- Esta etapa es fundamental para que los diferentes roles que toman parte en un proceso de desarrollo conozcan sus responsabilidades desde el punto de vista de la seguridad.



◆◆◇ El ciclo de desarrollo de *software* seguro

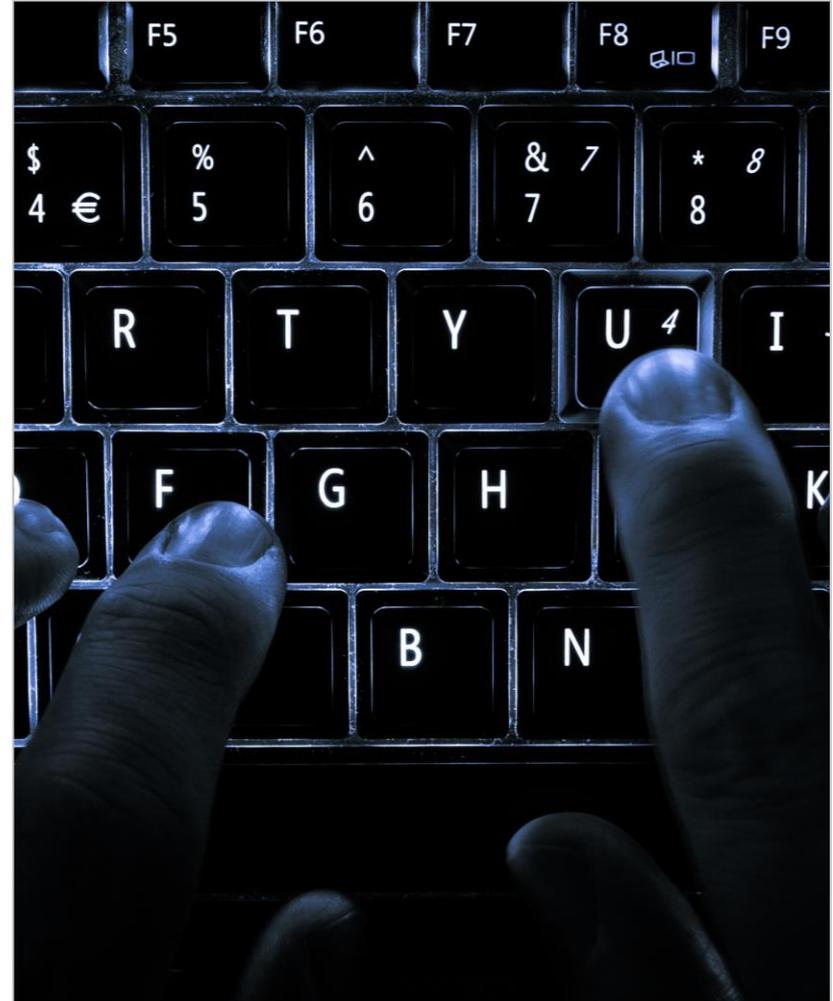
Requisitos

- Durante esta fase, además de los requisitos funcionales tradicionales de la aplicación se deben tener en cuenta los requisitos de seguridad, privacidad y regulatorios:
 - Se deben definir un conjunto mínimo de requisitos de seguridad.
 - Al igual que con el resto de requisitos, se deben implementar las medidas necesarias para poder trazar todo su desarrollo durante el SDLC.
- Otro mecanismo es definir un conjunto de métricas de seguridad que se deben mantener durante las diferentes fases del desarrollo:
 - Establecer niveles de severidad para vulnerabilidades.
 - Indicar por cada fase del desarrollo los niveles máximos aceptables.
 - Ej.: no se puede pasar a la fase de lanzamiento con alguna vulnerabilidad crítica.
- Para facilitar la identificación de requisitos se llevan a cabo estos procesos:
 - Identificar los roles, sus capacidades y los recursos de la aplicación.
 - Análisis de riesgos.
 - Definición de casos de abuso.

◆◆◆ El ciclo de desarrollo de *software* seguro

Diseño

- Durante esta fase se deben definir las soluciones de seguridad que cubrirán los requisitos de seguridad descritos en la fase anterior.
- Además, durante la fase de diseño se deberán especificar los detalles funcionales que no hayan sido especificados durante la fase de requisitos.
 - Ejemplo: algoritmos criptográficos a utilizar.
- El S-SDLC añade a la etapa de diseño del *software* un conjunto de principios que se deben seguir para el diseño del sistema. Estos principios deben tenerse en cuenta de forma transversal durante el diseño del sistema.



◆◆◇ El ciclo de desarrollo de *software* seguro

Diseño – Principios de diseño seguro I

- **Defensa en profundidad:**
 - Consiste en crear diferentes capas de seguridad, de tal forma que si una falla, el sistema no se vea comprometido.
 - Requiere diseñar distintas estrategias de defensa para una misma amenaza.
- **Fallo seguro:**
 - Consiste en que todos los fallos lleven a un estado del sistema que se considere seguro (sin pérdida de confidencialidad, integridad y disponibilidad).
- **Mínimo Privilegio:**
 - Cada usuario o proceso debe poseer sólo, los mínimos privilegios posibles para llevar a cabo las tareas que le son permitidas.
 - Los privilegios se deben otorgar por el mínimo tiempo posible.
- **Separación de privilegios:**
 - La consecución de cualquier actividad que se considere como crítica en el sistema debe requerir la participación de dos o más entidades.
 - Tiene como objetivo también eliminar los puntos únicos de fallo.

Diseño – Principios de diseño seguro II

- **Simplicidad:**
 - A mismo nivel de seguridad es preferible, por norma general, utilizar las soluciones menos complejas.
 - A mayor simplicidad, menor superficie de ataque en general.
- **Supervisión:**
 - Se debe comprobar durante la ejecución de cualquier tarea (acceso, escritura, modificación) que el usuario o proceso que la ejecuta está autorizado para ello.
 - Para evitar problemas de sincronización se recomienda no utilizar cachés de autorización.
- **Diseño abierto:**
 - Los detalles del diseño del sistema deben ser abiertos, evitando los casos de seguridad por oscuridad.
 - Este principio ayuda a crear sistemas seguros desde el diseño.
 - Este principio asegura que la publicación o revisión del diseño no impliquen de forma directa un incidente grave de seguridad.

◆◆◇ El ciclo de desarrollo de *software* seguro

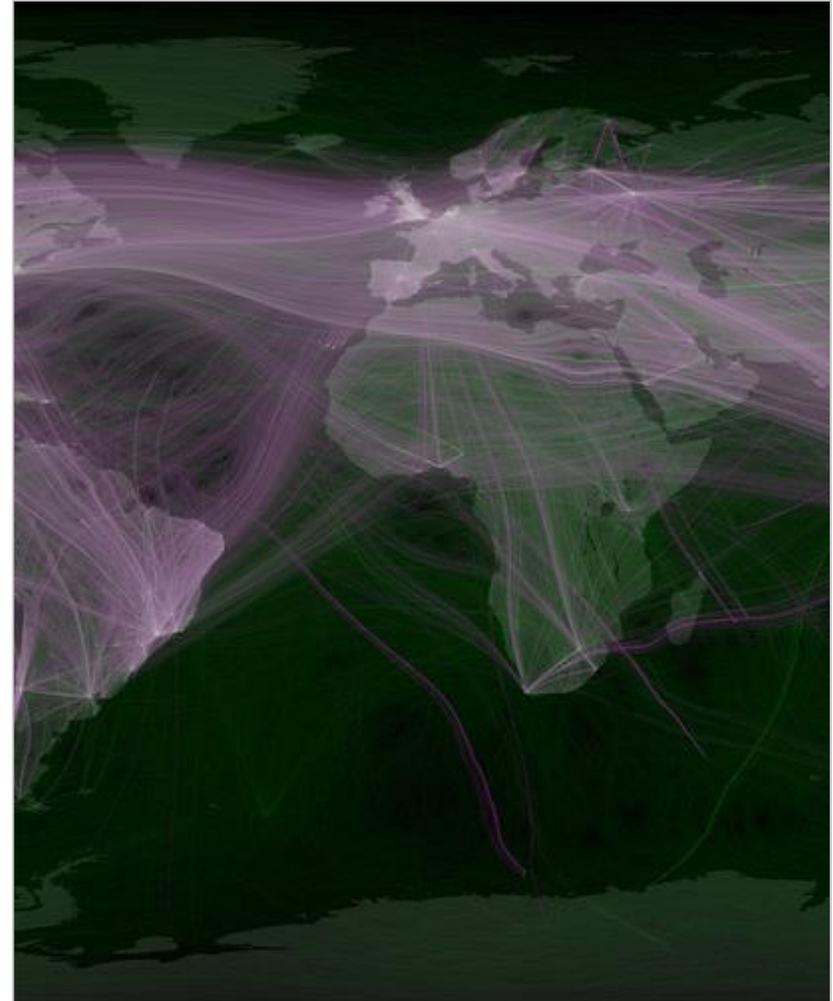
Diseño – Principios de diseño seguro III

- **Mínimo en común:**
 - Este principio desaconseja la utilización de un mismo mecanismo, aunque sea común a varios procesos o usuarios, si estos tienen diferentes niveles de privilegio.
- **Aceptabilidad:**
 - Los mecanismos de seguridad del sistema se deben diseñar teniendo en cuenta la aceptabilidad por parte de sus usuarios.
 - Si los usuarios tienen dificultades en usar las características de seguridad, buscarán mecanismos para saltárselas, haciéndolas inútiles.
- **Punto más débil:**
 - La seguridad de todo el sistema dependerá de su punto más débil.
- **Reutilización:**
 - Es preferible la utilización de componentes ya existentes y verificados que la creación de nuevos que puedan incrementar el riesgo de vulnerabilidades y superficie de ataque.

◆◆◆ El ciclo de desarrollo de *software* seguro

Diseño – Superficie de ataque

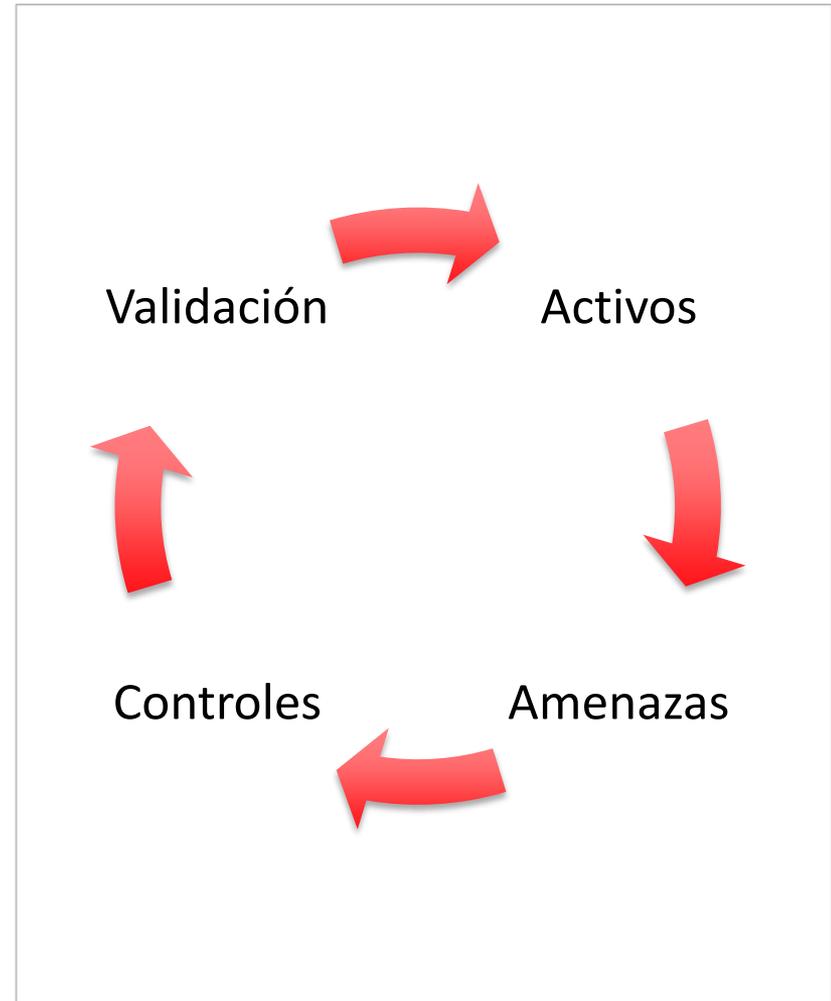
- Consiste en especificar, de manera estructurada, los puntos de entrada al sistema. Esta tarea debe ser realizada por el diseñador.
- Los puntos entrada de la aplicación pueden categorizarse en:
 - Red.
 - Sistema de ficheros.
 - Usuario.
- Para cada punto de entrada se deben identificar los:
 - Recursos a los que se puede acceder a través del mismo.
 - Roles que tienen acceso al punto de acceso.
- Permite identificar fugas de recursos a roles que no deberían tener los privilegios necesarios.



◆◆◇ El ciclo de desarrollo de *software* seguro

Diseño – Modelado de amenazas

- Tal y como se estudió durante la unidad 3, se catalogan y evalúan los diferentes riesgos y amenazas a los que puede estar sometido un sistema.
 - Será la primera tarea realizada por cualquier atacante.
 - No efectuarlo reduce nuestra capacidad de protección.
- Amenaza != vulnerabilidad. Las amenazas son persistentes.
- El modelado de amenazas es un proceso iterativo que consiste en:



◆◆◇ El ciclo de desarrollo de *software* seguro

Diseño – Modelado de amenazas

- Identificar los activos o capacidades existentes en el sistema mediante un diagrama. Es importante comprobar si coinciden con los definidos en la documentación.
- Por cada activo o capacidad identificar las amenazas potenciales.
 - Esta tarea requiere de cierta creatividad por parte del analista.
- Por cada amenaza evaluar el riesgo existente:
 - Utilizar árboles de amenazas que describan los distintos pasos que debe llevar el atacante para materializarla.
 - Medir factores como: impacto, reproducibilidad, explotabilidad y usuarios afectados.
- Por cada amenaza identificar los controles que sea factible implementar para su mitigación.
- Al final del proceso, deberían quedar cubiertos el mayor número de amenazas posibles.

◆◆◆ El ciclo de desarrollo de *software* seguro

STRIDE

- STRIDE es un modelo de amenazas que agrupa las mismas en 6 categorías:
 - **Spoofing** (Suplantación): suplantar la identidad de un sistema o usuario.
 - Ejemplo: intentar actuar como administrador del sistema.
 - **Tampering** (Manipulación): modificar los datos o el código.
 - Ejemplo: modificar el código fuente de la aplicación para desactivar protecciones.
 - **Repudiation** (Repudio): denegar que se ha realizado una acción específica.
 - Ejemplo: “Yo no envíe ese mensaje”.
 - **Information Disclosure** (Fuga de información): acceso a una pieza de información por parte de una entidad sin credenciales para ello.
 - Ejemplo: información personal filtrada al público.
 - **Denial of Service** (Denegación de servicio): bloquear o degradar un servicio.
 - Ejemplo: bloqueo de servidores por un conjunto alto de peticiones.
 - **Elevation of Privilege** (Elevación de privilegios): incrementar las capacidades sin la autorización apropiada.
 - Ejemplo: paso de usuario a administrador.

◆◆◇ El ciclo de desarrollo de *software* seguro

STRIDE - Controles

- Frente a este tipo de amenazas se establecen los siguientes controles sobre el desarrollo, para mitigar el posible impacto de una brecha de seguridad.

Amenaza	Control/Servicio de seguridad
Suplantación	Autenticación
Manipulación	Controles de Integridad
Repudio	Métodos de no repudio
Fugas de información	Mecanismos de confidencialidad
Denegación de servicio	Disponibilidad
Elevación de privilegios	Autorización

◆◆◇ El ciclo de desarrollo de *software* seguro

Implementación

- En el SDLC tradicional esta fase conlleva la codificación de las diferentes funciones del producto *software* a desarrollar.
- Las actividades del S-SDLC tienen como objetivo ayudar a los desarrolladores a implementar las funcionalidades requeridas de la forma más segura posible.
- La principal aportación del S-SDLC a esta fase son las guías y buenas prácticas de codificación segura (se verán en más detalle en las siguientes secciones).
- Además, durante la etapa de implementación, un S-SDLC debe considerar las siguientes actividades:
 - Configuración segura del entorno de desarrollo.
 - Revisión de código fuente de la aplicación.
 - Revisión de elementos de terceros.



◆◆◇ El ciclo de desarrollo de *software* seguro

Implementación – Entorno de desarrollo seguro

- Se debe definir una configuración oficial para el entorno de desarrollo a utilizar durante la implementación del producto *software*.
- La configuración debe especificar:
 - Sistema o sistemas operativos válidos (con versiones).
 - Herramientas soportadas para el desarrollo (con versiones):
 - IDE.
 - Sistemas de control de versiones.
 - Restricciones para el acceso remoto.
- Se deben incluir los mecanismos necesarios para aplicar y restringir la configuración de las estaciones de trabajo a la aceptada:
 - Restricciones a cuentas de usuario.
 - Entornos pre-instalados.

◆◆◇ El ciclo de desarrollo de *software* seguro

Implementación – Entorno de desarrollo seguro

- Un ejemplo muy claro de los problemas que puede ocasionar no seguir estas directrices es [XcodeGhost](#).
- Un conjunto de ciber-delincuentes modificó y puso a disposición pública (en un servidor chino) una versión del IDE XCode para iOS y Mac OS.
- La modificación inyectaba código malicioso en la versión compilada de aplicaciones de iOS.
- Debido a la lentitud de la descarga desde servidores de Estados Unidos, muchos desarrolladores chinos optaron por descargar la versión disponible en los servidores de su país.
- Al utilizar la versión modificada para desarrollar sus aplicaciones, sin tener conocimiento de ello, muchos desarrolladores crearon aplicaciones maliciosas que fueron publicadas en la App Store.
 - <https://developer.apple.com/news/?id=09222015a>
 - [https://www.incibe.es/technologyForecastingSearch/CERT/Bitacora de ciberseguridad/ataque_appstore](https://www.incibe.es/technologyForecastingSearch/CERT/Bitacora_de_ciberseguridad/ataque_appstore)

◆◆◇ El ciclo de desarrollo de *software* seguro

Implementación – Revisión de código I

- La revisión del código fuente de la aplicación permite identificar vulnerabilidades que se introducen durante la fase de implementación.
- Las herramientas automáticas de análisis estático como las estudiadas durante la unidad 3 facilitan esta tarea, pero no son capaces de encontrar ciertas vulnerabilidades que necesitan una revisión manual.
- La revisión del código es una tarea adicional a la ejecución de los diferentes pruebas unitarias y de integración que se definen dentro del SDCL tradicional. En ningún momento es equivalente, ni debe sustituirlos.
- La revisión de código fuente se puede realizar:
 - De forma ligera durante el proceso de implementación.
 - De manera formal una vez se ha finalizado una parte del proceso de implementación.

◆◆◇ El ciclo de desarrollo de *software* seguro

Implementación – Revisión de código II

- En cuanto a las revisiones ligeras del código fuente, se pueden realizar de las siguientes maneras:
 - **Técnicas de *pair-programming*:** dos personas se encargan de desarrollar código juntos en la misma máquina, supervisando el código escrito mutuamente.
 - **Revisión externa:** el autor explica el código a otro desarrollador que se encarga de la verificación del mismo.
 - **Revisión asistida:** se utilizan herramientas semi-automáticas que permiten, durante la programación, identificar problemas en el código.
 - **Revisión por “commit”:** cada vez que se efectúa un “commit” en el sistema de control de versiones se lanza una herramienta que:
 - Envía el elemento por correo a los revisores de forma automática.
 - Realiza un análisis del mismo a través una herramienta de análisis integrada con el control de versiones.
 - Ejemplo: <https://www.pullreview.com/> o <https://codeclimate.com/>

◆◆◇ El ciclo de desarrollo de *software* seguro

Implementación – Elementos de terceros

- Durante la fase de implementación, es posible que sea necesario utilizar herramientas y librerías de terceros.
- Los controles que se realizan sobre nuestro propio código deben ser también implementados sobre este tipo de librerías.
- En concreto se deben realizar las siguientes tareas:
 - Si el código fuente está disponible, someterlo a un proceso de análisis de código fuente como el descrito anteriormente.
 - Revisar las vulnerabilidades o posibles problemas de seguridad asociados a la versión de la librería que estamos utilizando:
 - Almacenamiento seguro.
 - Comunicaciones cifradas.
 - Validación de datos de entrada.
 - Problemas de configuración o exposición de datos por defecto.
 - Comprobar la utilización de funciones o elementos que han sido declarados como obsoletos (*deprecated*) por los desarrolladores.

◆◆◇ El ciclo de desarrollo de *software* seguro

Verificación

- En el SDLC tradicional esta fase incluye todas las actividades encaminadas a comprobar que el producto *software* funciona como está descrito en los requerimientos.
- Las tareas del S-SDLC en la etapa de verificación permiten realizar las comprobaciones de seguridad directamente sobre elementos de *software* que se han implementado en la etapa anterior:
 - **Análisis dinámico:** estudiado en la Unidad 3. Permite verificar las propiedades de seguridad del sistema y su comportamiento mediante su ejecución.
 - **Fuzzing:** es parte del análisis dinámico. Se comprueba si los controles implementados en los puntos de entrada en el sistema controlan correctamente las diferentes entradas posibles.
 - **Revisión de la superficie de ataque:** una vez terminado el código se puede verificar que la superficie de ataque real se ajusta a la identificada en las etapas anteriores del S-SDLC.

◆◆◇ El ciclo de desarrollo de *software* seguro

Despliegue I

- Durante esta fase se prepara el producto *software* para su lanzamiento.
- En lo relativo al S-SDLC, esta fase incluye actividades para cubrir los aspectos de seguridad del producto más allá de su fecha de lanzamiento.
- Plan de respuesta ante incidentes:
 - Permite mitigar el alcance de incidentes de seguridad, reducir el riesgo y los costes de un incidente.
 - Debe identificar de forma clara los eventos que considerar para declarar la existencia de un incidente de seguridad.
 - Por cada incidente se identificarán de forma detallada las acciones a tomar.
 - Se deben incluir los roles de cada miembro del equipo de respuesta y su información de contacto.
 - Esta tarea es fundamental para poder responder con celeridad ante cualquier incidente de seguridad.
 - El plan de respuesta no es un documento estático. Evoluciona según se modifica el sistema o aparecen nuevas amenazas no tenidas en cuenta.

Despliegue II

- **Revisión de seguridad final:**
 - Antes del lanzamiento, se debe verificar que todas las tareas de seguridad planeadas para llevar a cabo el S-SDLC se han completado.
 - Además, conviene realizar una revisión de cada una de las tareas realizadas para asegurar que no se ha cometido ningún fallo durante las mismas.
- **Certificación:**
 - Permite asegurar que el producto cumple con ciertas normativas/regulaciones de seguridad.
- **Archivado:**
 - Consiste en guardar una copia de todos los elementos envueltos en la versión del *software* que va a ser lanzada.
 - Será uno de los elementos a considerar en caso de incidente de seguridad.
- Tareas como análisis dinámico, *fuzzing* y otras revisiones de seguridad se siguen ejecutando durante esta etapa.

◆◆◆ El ciclo de desarrollo de *software* seguro

Respuesta

- Esta fase sólo se activa en respuesta a sucesos que hayan sido declarados como generadores de un incidente en el plan de respuesta ante incidentes.
- Una vez activado se deben seguir las directrices marcadas por el plan, incluidos:
 - Personal al que notificar y orden de notificación.
 - Captura de datos para el análisis posterior del incidente.
 - Ejecución de tareas de mitigación de la amenaza.
 - Ejecución de tareas para el restablecimiento del servicio (en caso de que sea necesario).



A close-up photograph of a person's hands typing on a laptop keyboard. The person has red nail polish. The laptop is dark-colored. In the foreground, there is a pair of black-rimmed glasses and an orange pen with silver accents. The background is blurred, showing white flowers with yellow centers. A semi-transparent grey rectangular box is overlaid on the center of the image, containing white text.

El S-SDLC en entornos de desarrollo ágiles

◆◆◇ El S-SDLC en entornos de desarrollo ágiles

- Las metodologías ágiles son un proceso alternativo a las metodologías tradicionales que se basan en el desarrollo a través de iteraciones más pequeñas para incorporar funcionalidad (<http://agilemethodology.org>).
- Las tareas y actividades que establece habitualmente el S-SDLC, asumen el ciclo de vida tradicional (cascada) durante el desarrollo del *software*.
- Generalmente, los sistemas y productos desarrollados para entornos móviles son desarrollados mediante metodologías ágiles.
- La ejecución del S-SDLC y tal como lo hemos visto, requiere de adaptaciones para poder aplicarse sobre metodologías ágiles.
- En estos casos, las actividades del S-SDLC se ejecutan con tres frecuencias diferentes:
 - Por **sprint**: aquellas actividades que se deben ejecutar por cada *release* que se complete.
 - Por **bucket**: aquellas actividades que se deben ejecutar por cada conjunto de *sprints*.
 - Por **proyecto**: las actividades que se ejecutan una sola vez en todo el proyecto.

◆◆◆ El S-SDLC en entornos de desarrollo ágiles

- **Actividades por *sprint*:**
 - Modelado de amenazas de la funcionalidad incluida en el *sprint*.
 - Todas las relacionadas con la fase de implementación del S-SDLC.
 - Revisión de seguridad final por *sprint*.
 - Certificación y archivado.
- **Actividades por *bucket*:**
 - Definir las métricas de seguridad con las que se evaluará el *bucket*.
 - Tareas de análisis dinámico, *fuzzing* y revisión de la superficie de ataque.
- **Actividades por proyecto:**
 - Definir los requisitos de seguridad.
 - Análisis de riesgos.
 - Definir la superficie de ataque.
 - Crear un plan de respuesta ante incidentes.

A hand is visible in the lower-left corner, pointing towards the center. The background is a dark, textured surface with glowing blue and green digital elements. The words "infected" and "payload" are prominently displayed in a pixelated, digital font. A semi-transparent blue rectangle is overlaid on the center, containing the main title text.

Buenas prácticas en el desarrollo seguro

◆◆◇ Buenas prácticas en el desarrollo seguro

Introducción

- Durante la anterior sección se han estudiado las diferentes fases y actividades que envuelven un S-SDLC.
- Durante esta sección vamos a estudiar una serie de guías y prácticas generales para la codificación segura de aplicaciones.
- Estas guías son independientes del lenguaje de programación y la plataforma para la que se desarrolla.
- En el caso de desarrollo de aplicaciones móviles deben utilizarse donde corresponda ya sea el *back-end* o el *end-point* (aplicación móvil).
- Su objetivo es ofrecer al desarrollador un conjunto de prácticas para poder implementar *software* de forma segura sin la necesidad de conocer en profundidad conceptos relativos a la seguridad y explotación de vulnerabilidades.
- El seguimiento de unas buenas prácticas de codificación segura no es suficiente para afirmar que se está llevando a cabo un S-SDLC, es sólo una parte de todo el proceso.

◆◆◆ Buenas prácticas en el desarrollo seguro

Listado

- El conjunto de prácticas que se estudiarán en esta sección incluye:
 - Validación de entrada.
 - Codificación de los elementos de salida.
 - Autenticación y gestión de contraseñas.
 - Gestión de sesiones.
 - Control de acceso.
 - Gestión de errores.
 - Protección de datos.
 - Seguridad en las comunicaciones.
 - Configuración del sistema.
 - Seguridad en la base de datos.
 - Gestión de memoria.
 - Otras consideraciones generales.



◆◆◇ Buenas prácticas en el desarrollo seguro

Validación de entrada I

- Toda entrada al sistema debe considerarse como maliciosa (*All input is evil*):
 - Campos de texto.
 - URL.
 - *Cookies* y otros campos HTTP.
- La validación de los datos de entrada debe llevarse a cabo siempre en un sistema que sea considerado fiable, generalmente el *back-end*. El dispositivo móvil no se puede considerar como elemento confiable.
- Toda la validación de los datos debe centralizarse en un punto de la aplicación.
- Antes de realizar la validación de los datos, es recomendable unificar la codificación de los mismos para que todas las comprobaciones se realicen con la misma codificación.

◆◆◆ Buenas prácticas en el desarrollo seguro

Validación de entrada II

- Para ello se recomienda:
 - Validar los rangos y longitud de los datos.
 - Utilizar listas blancas para comprobar que todos los elementos de una entrada son válidos.
 - Validar que los tipos de datos que se reciben concuerdan con los esperados:
 - Las cabeceras HTTP deben contener solo caracteres ASCII.
 - Si se espera una imagen en un formato específico comprobar que se recibe ese formato.
 - Los campos de texto y parámetros de la URL deben contener el tipo de dato que se espera en la aplicación.
- En caso de que existan caracteres o cadenas que puedan considerarse como peligrosos < > ../ ..\ % \ () “ ‘ \’ \” se deberán añadir controles adicionales específicos para las llamadas que pueden incluirlos.
 - En el caso de entradas que sean interpretables (como código HTML) evitar la utilización de redirecciones que puedan hacer los controles inefectivos.

◆◆◆ Buenas prácticas en el desarrollo seguro

Codificación de los elementos de salida

- Al igual que la validación de entrada, la codificación de los datos de salida se debe efectuar en un sistema confiable como el *back-end* de la aplicación.
- Se debe evitar reinventar la rueda. Existen múltiples librerías y métodos de codificación de salida ampliamente testeados y aceptados por la comunidad:
 - En iOS se puede utilizar el método `stringByAddingPercentEncodingWithAllowedCharacters` de la clase `NSString`.
 - En Android se puede utilizar [URLEncoder](#) o [DatabaseUtils](#).
- Los datos de salida se deben codificar dependiendo del uso que se va a hacer de ellos en la aplicación:
 - En caso de que la salida vaya a ser interpretada por un navegador web, evita que se puedan generar elementos interpretables en HTML, CSS, Javascript etc.
 - Si la salida va a ser interpretada por otro sistema hay que evitar que se puedan formar o modificar los comandos a los mismos (SQL, XML, LDAP, etc.).

◆◆◇ Buenas prácticas en el desarrollo seguro

Autenticación y gestión de contraseñas I

- Todas las páginas, excepto aquellas que se definan estrictamente como públicas, deben requerir autenticación por parte de los usuarios.
- Para la implementación de los controles de autenticación se identifican las siguientes recomendaciones:
 - Los controles de autenticación se deben llevar a cabo siempre en un sistema fiable (*back-end*).
 - Todos los controles de autenticación deben estar centralizados en un único módulo, incluidas aquellas librerías que puedan realizar llamadas a servicios de autenticación externos.
 - La lógica de autenticación no debe estar acoplada a la lógica del recurso al que se accede.
 - Las peticiones de autenticación se deben realizar siempre mediante conexiones HTTP POST cifradas convenientemente (SSL).

Autenticación y gestión de contraseñas II



- Para el proceso de autenticación se recomiendan las siguientes prácticas:
 - La validación de los datos de autenticación se debe llevar a cabo sólo si se han introducido todos los datos necesarios para llevarla a cabo (usuario y contraseña).
 - En caso de que se produzca un fallo de autenticación, no se deben ofrecer detalles, ni visuales, ni en el código fuente utilizado, sobre el fallo concreto en la autenticación (contraseña errónea, usuario erróneo, etc.).
 - El proceso de autenticación debe fallar de forma segura.
 - Independientemente del método de acceso, el campo para la introducción de la contraseña no debería mostrar los elementos tecleados.

◆◆◇ Buenas prácticas en el desarrollo seguro

Autenticación y gestión de contraseñas III

- Bajo ningún concepto se deben guardar las contraseñas de la aplicación en claro.
- Todas las contraseñas deben almacenarse resumidos mediante una función criptográficamente segura, utilizando un salt para dificultar los ataques de fuerza bruta mediante *rainbow tables*.
- La aplicación debe obligar a los usuarios a utilizar contraseñas con un mínimo de complejidad:
 - Longitud mínima de 8 caracteres, pero más son recomendados.
 - Caracteres alfanuméricos, signos de puntuación y números.
- Si la aplicación genera contraseñas por defecto, obligar al usuario a cambiarla en el primer acceso.
- Si se realizan varios intentos fallidos de acceso desactivar el mismo durante un periodo de tiempo que sea lo suficientemente largo como para evitar ataques de fuerza bruta, pero no para provocar denegación de servicio al usuario.

Autenticación y gestión de contraseñas IV

- En cuanto al restablecimiento de contraseñas:
 - Siempre que sea posible, se debe evitar la utilización de preguntas de seguridad. En el caso de que sean necesarias, se deben evitar preguntas cuya respuesta sea predecible o común:
 - Ej. incorrecto: ¿Cuál es el nombre de tu primera mascota?
 - Ej. correcto: ¿Calle en la que creció tu madre?
 - Se debe comprobar que el correo al que se envía una solicitud de restablecimiento está registrado en el sistema.
- En caso de que el usuario quiera efectuar alguna operación crítica en el sistema como por ejemplo el propio cambio de contraseña, se deberá volver a autenticar al usuario.
- Si es posible, implementar un doble factor de autenticación mediante:
 - Contraseña + aplicación móvil que genere *passwords* de un solo uso ([Google authenticator](#)).
 - Contraseña + elemento biométrico.

◆◆◇ Buenas prácticas en el desarrollo seguro

Gestión de sesiones

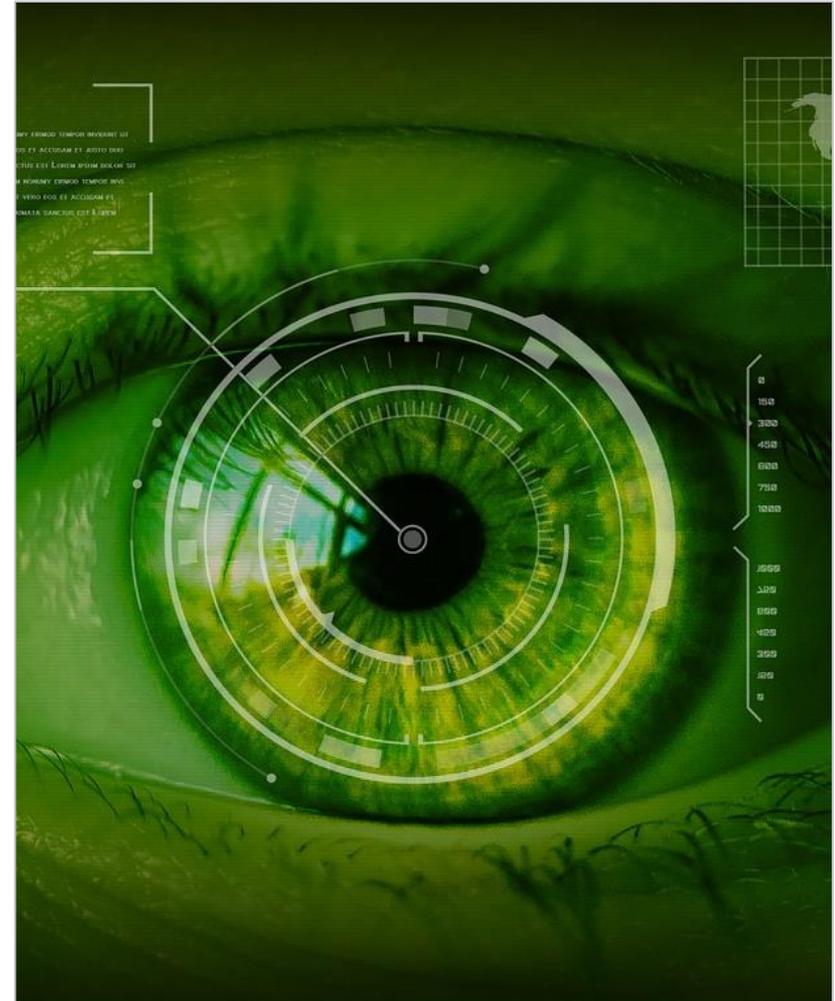
- Conviene utilizar, si ofrece las suficientes garantías, el control de sesiones que incorpora el servidor framework en el que se desarrolla la aplicación:
 - [iOS](#)
 - [Android](#)
 - [Java EE](#)
 - [.Net](#)
 - [Django](#)
 - [Ruby on Rails](#)
- Los identificadores deben ser creados por un sistema confiable (generalmente el *back-end*) con librerías que aseguren que son lo suficientemente aleatorios.
- Cada re-autenticación debería generar un nuevo identificador de sesión y eliminar el anterior activo.
- El usuario debe tener la posibilidad de cerrar una sesión de forma sencilla.
- Toda sesión debería expirar tras un periodo mínimo de inactividad.
- Se debe evitar exponer la información sobre la sesión o cookies a terceros: registro de *logs*, utilización de parámetros GET, etc.
- Dependiendo de las limitaciones de presupuesto, se debe ofrecer un sistema al usuario que permita el control y cerrado de sesiones activas.

◆◆◆ Buenas prácticas en el desarrollo seguro

Control de acceso

- Las decisiones de control de acceso deben ser tomadas en base a información que provenga de sistemas confiables.
- Al igual que con la validación de entrada, salida y autenticación, conviene que el sistema de control de acceso esté centralizado y separado del resto de la lógica, en un único elemento del sistema.
- El control de acceso se deber realizar para todas las peticiones, incluidas aquellas que se hagan mediante tecnologías como AJAX.
- Los usuarios que no están autorizados, no deben poder acceder a elementos como:

- Datos de la aplicación y servicios.
- URL que sean accesibles sólo por



◆◆◆ Buenas prácticas en el desarrollo seguro

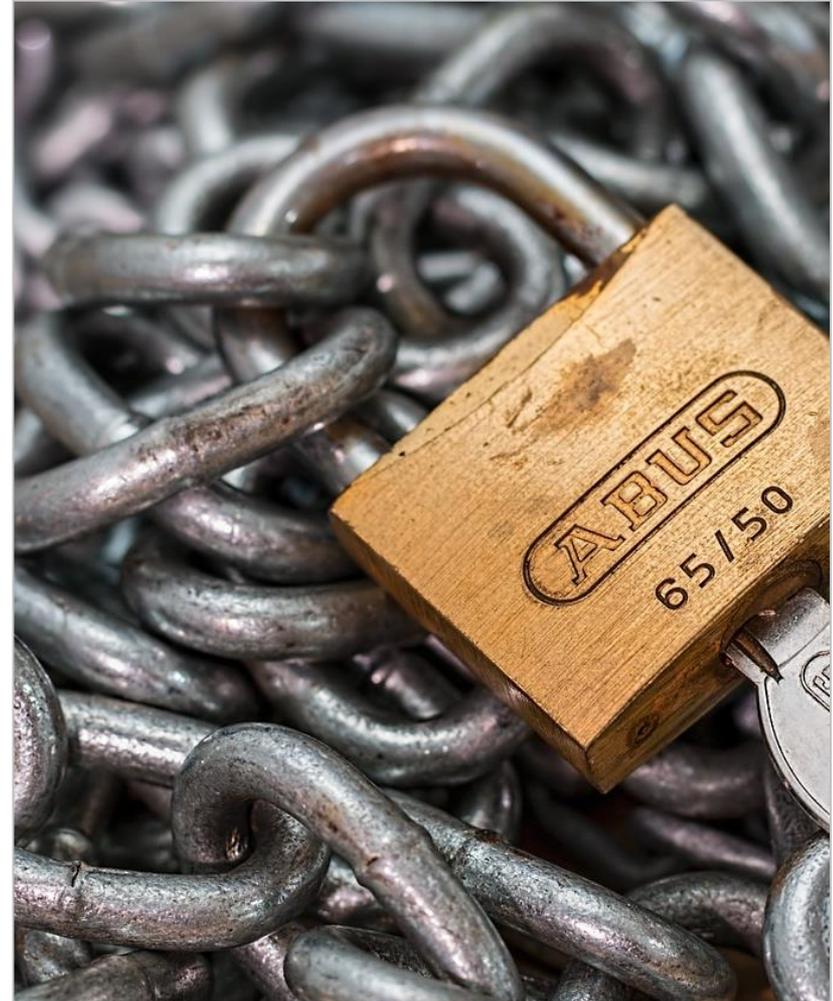
Gestión de errores

- Ante la aparición de un error se debe evitar revelar información sensible como detalles del sistema, identificadores de sesión o información sobre cuentas.
- La aplicación debería manejar todos los errores y no depender nunca de los errores por defecto del sistema.
- Ante la aparición de un error, la política por defecto de cara a la tarea que se está realizando debe ser la denegación.
- Los *logs* deben registrar los sucesos relevantes en el sistema:
 - Fallos en la validación de entrada.
 - Intentos de autenticación fallidos.
 - Intentos de conexión con sesiones expiradas.
 - Cambios en la configuración de elementos críticos.
 - Excepciones en el sistema y otros errores ocurridos durante la ejecución.

◆◆◆ Buenas prácticas en el desarrollo seguro

Protección de datos

- Las contraseñas, *tokens* de autenticación y otra información sensible deben almacenarse cifrados.
- Se debe evitar bajo todos los medios almacenar credenciales dentro del propio código fuente de la aplicación o en archivos de configuración. En el caso de utilizar repositorios abiertos como GitHub se podrían estar publicando las credenciales de acceso a los servicios.
- Configura el servidor de aplicaciones para que los ficheros del código fuente de la aplicación *back-end* no se puedan descargar.
- Elimina los ficheros de documentación y configuración que



◆◆◆ Buenas prácticas en el desarrollo seguro

Seguridad en las comunicaciones

- Dado que la mayoría de conexiones para acceder a los servicios de la aplicación incluirán tokens de autenticación, sesiones o información sensible, las conexiones entre los diferentes clientes y el servidor deben realizarse cifradas.
- Las aplicaciones deben verificar la validez del certificado que se les presenta e incluso utilizar técnicas de “*certificate pinning*” para mitigar ataques al sistema de PKI.
- Los recursos accesibles a través de conexiones seguras no deben estar disponibles a través de conexiones que no lo son (*downgrade* a conexiones sin cifrar).
- La implementación de estas tecnologías en aplicaciones móviles se verá con más detalle en la siguiente



◆◆◇ Buenas prácticas en el desarrollo seguro

Configuración del sistema

- Asegurarse de que las versiones que se están ejecutando de los diferentes elementos de terceros que se requieren para la ejecución de la aplicación son las aprobadas durante el diseño.
- Es necesario también revisar que durante el proceso de desarrollo no se haya registrado ninguna vulnerabilidad que afecte a las versiones aprobadas. En ese caso se deberán revisar y escoger de nuevo.
- El sistema en producción no debe contener los ficheros de código fuente y recursos que hayan sido utilizados para efectuar los diferentes *tests* y verificaciones durante el proceso de desarrollo.
- En caso de que parte de la aplicación sea ofrecida por un servidor web, utilizar el correspondiente fichero "*robots.txt*" para evitar el indexado. Hay que tener cuidado con este punto, ya que podemos ofrecerle información extra al atacante.
- Es recomendable que durante el desarrollo del *software* se utilice un sistema para el control de versiones.

Seguridad en la base de datos

- El acceso a la base de datos debe realizarse, independientemente del tipo de base de datos, mediante consultas parametrizadas.
- Los parámetros utilizados, y resultados obtenidos en las consultas deben pasar por sus correspondientes procesos de codificación y validación (escapado y filtrado).
- Las diferentes aplicaciones y sistemas deben utilizar el menor nivel de privilegios posibles para acceder a las tablas de la base de datos.
- Los roles con diferentes niveles de acceso deben acceder mediante usuarios diferentes para asegurar la separación de privilegios.
- La conexión a la base de datos debe mantenerse durante el tiempo estrictamente necesario para completar las solicitudes que se requieran.
- Al igual que con el resto de subsistemas (servidor de aplicaciones, etc.) se deben eliminar todos los ficheros y configuración de la instalación por defecto que no sean necesarios.

◆◆◇ Buenas prácticas en el desarrollo seguro

Gestión de memoria I

- Algunos lenguajes de programación se encargan de la gestión de memoria de forma automática a través de sus entornos de ejecución (Java, Javascript, Python, Swift, etc.) pero otros como C (que se puede utilizar para el desarrollo de aplicaciones móviles en Android o iOS) tienen un sistema de gestión de memoria manual.
- En aquellos casos es fundamental llevar a cabo una buena gestión de la misma. La mayoría de vulnerabilidades críticas se deben a problemas de gestión de memoria (desbordamiento de búfer).
- Los puntos más críticos en lo referente a la gestión de memoria son aquellos en los que:
 - Se realizan copias de búferes entre direcciones de memoria.
 - Se reserva espacio en memoria para variables de longitud no definida.
 - Se libera memoria previamente liberada.

Gestión de memoria II

- Es conveniente seguir una serie de pautas que limiten al máximo la aparición de problemas de gestión de memoria:
 - Cuando se utilicen funciones que acepten el número de bytes a copiar (como `strncpy`) se debe tener en cuenta que el búfer de destino puede no finalizar en cero (no se copie hasta el último byte de origen).
 - Cuando se realizan copias entre búferes, se debe comprobar que los tamaños concuerdan y que no existe la posibilidad de escribir pasado el espacio reservado a cada búfer (condición de fin de copia bien definido).
 - Se deben definir tamaños máximos para todos los búferes utilizados.
 - Una vez no se necesita una variable para la que se ha reservado memoria, se debe liberar o cerrar el recurso. No se debe confiar en la labor del recolector de basuras.
 - Siempre que sea posible, hay que evitar la utilización de funciones peligrosas como `strcat`, `strcpy`, etc.

◆◆◇ Buenas prácticas en el desarrollo seguro

Otras consideraciones generales I

- Independientemente del aspecto a programar, si ya existe código testeado y verificado que realice esa operación, siempre es mejor la reutilización.
- Siempre que haya que realizar una tarea relacionada con el sistema operativo, se debe ejecutar a través de las API ofrecidas por el mismo. En ningún caso se deben enviar comandos directamente al sistema operativo a través de la consola.
- Siempre que se vaya a ejecutar código que no haya sido incluido en el despliegue inicial de la aplicación (ejecución dinámica) se debe verificar la integridad del mismo.
- Se deben utilizar los mecanismos de sincronización existentes en el sistemas operativo para evitar la aparición de condiciones de carrera.
- Todas las variables y fuentes de datos deben ser inicializadas antes de su primer uso.

◆◆◆ Buenas prácticas en el desarrollo seguro

Otras consideraciones generales II

- Se debe tener en cuenta la representación numérica del lenguaje de programación para evitar errores en la realización de cálculos.
 - En concreto se debe tener en cuenta la precisión de las operaciones, tipos de datos con/sin signo, conversiones, castings y cómo el lenguaje de programación trata los números por encima y por debajo de los límites de representación.
- Si la aplicación va a implementar mecanismos de actualización automática, se debe revisar que el código recibido durante la misma procede de una fuente confiable.
 - Para ello se pueden utilizar mecanismos de firma de código como los utilizados en las tiendas de aplicaciones móviles. Una vez descargado el código y antes de la actualización se debe verificar la firma del mismo.



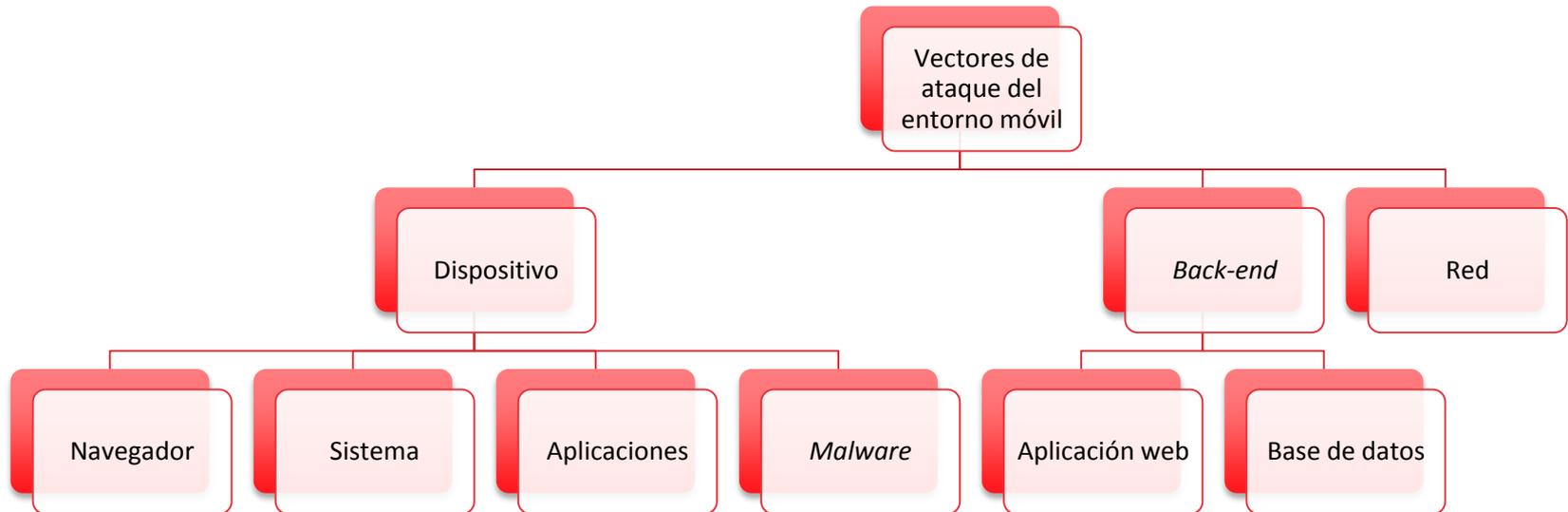
Buenas prácticas en el desarrollo móvil



◆◆◆ Buenas prácticas en el desarrollo móvil

Introducción

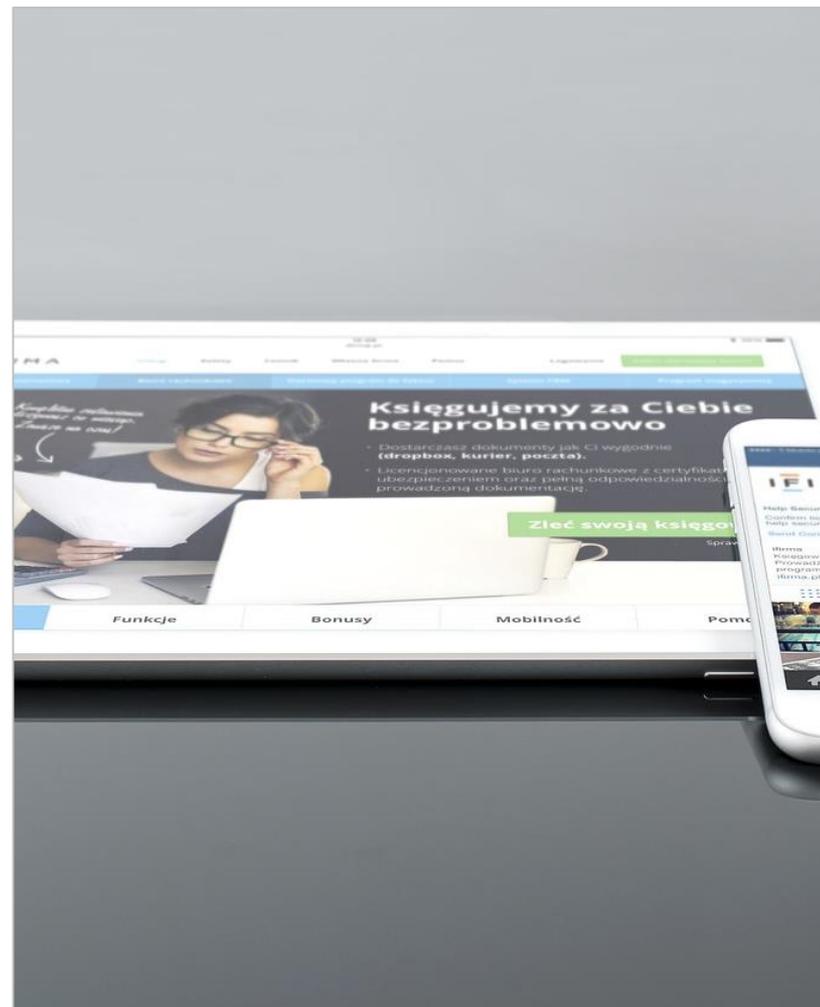
- Las aplicaciones móviles comparten características con las aplicaciones web (muchos usuarios, desarrollo rápido, conectividad continua a la red) y con los sistemas de escritorio (almacenamiento compartido de datos, *malware*, existencia de aplicaciones vulnerables como el navegador) en un entorno de movilidad.
- La superficie de ataque en un dispositivo móvil es una combinación de los elementos que afectan a ambos tipos de aplicación.



◆◆◆ Buenas prácticas en el desarrollo móvil

Aspectos específicos

- Durante el resto de la sección se van a estudiar los aspectos de seguridad, que hay que tener en cuenta durante el desarrollo de aplicaciones para mitigar las amenazas que generan los diferentes vectores de ataque del entorno móvil:
 - Protección del código de la aplicación.
 - Manejo de datos sensibles.
 - Logs y filtrado de información sensible.
 - Manejo de datos sensibles.
 - Componentes HTML en aplicaciones móviles.
 - Comunicación entre aplicaciones.
 - Autenticación en aplicaciones móviles.



A wooden mannequin figure is leaning over a black computer keyboard. A heavy metal chain is wrapped around the keyboard, and a large, clear plastic padlock is attached to the chain, locking it. The mannequin's head is positioned above the padlock, as if inspecting or guarding it. The background is a plain, light-colored wall.

Protección de la aplicación

◆◆◇ Protección de la aplicación

Ofuscación del código

- Como se comprobó durante la unidad 3 del curso, las técnicas de ingeniería inversa pueden ofrecer información muy valiosa sobre el funcionamiento de una aplicación.
- Incrementar la complejidad del código mediante la utilización de técnicas de ofuscación dificultará que el atacante pueda identificar vulnerabilidades y fallos que hayan pasados desapercibidos durante los distintos procesos de revisión.
 - [ProGuard](#)
 - [DexProtector](#)
- Para dificultar las tareas de ingeniería inversa se pueden utilizar las siguientes técnicas:
 - Restringir el uso de depuradores.
 - Detección de trazas.
 - Optimizaciones del depurador.
 - Destrucción de información de símbolos del binario.

◆◆◆ Protección de la aplicación

Restricción del uso de depuradores



- Las aplicaciones pueden restringir, a través del sistema operativo, el uso de depuradores para inspeccionar su ejecución.
- Si bien estas técnicas pueden ser burladas mediante técnicas de *repackaging*, requiere al atacante la realización de un esfuerzo extra.
- En Android, se puede especificar mediante el atributo `android:debuggable="false"` en la etiqueta de la aplicación dentro del *manifest*.
- En iOS se puede introducir la siguiente llamada durante el inicio en la ejecución de la aplicación para que se cierre en caso de que se intente añadir un depurador a la misma:
 - `ptrace(PT_DENY_ATTACH, 0, 0, 0);`

◆◆◇ Protección de la aplicación

Detección de trazas

- Dado que se pueden utilizar técnicas de *repackaging* para depurar la aplicación, conviene añadir controles para comprobar si la misma está siendo depurada.
- Si se detecta que la aplicación está conectada a un depurador, se puede:
 - Notificar al *back-end*.
 - Borrar los datos sensibles de la aplicación.

- En Android se puede identificar ejecutando la siguiente línea:

```
boolean depuracion= ( 0 != ( getApplicationInfo().flags &
ApplicationInfo.FLAG_DEBUGGABLE ) );
```

- En iOS se puede implementar el siguiente código ofrecido por Apple:

https://developer.apple.com/library/ios/qa/qa1361/_index.html

◆◆◇ Protección de la aplicación

Optimizaciones del depurador

- Las optimizaciones del depurador modifican el código para que sea más rápido en su ejecución en el procesador, pero también dificultan su lectura y comprensión.
- En Android, se pueden llevar a cabo dos alternativas:
 - Se puede programar parte de la aplicación en C para su utilización como librerías nativas.
 - ProGuard elimina el código no utilizado en la aplicación y modifica los nombres de los métodos, variables, clases y paquetes para dificultar su comprensión. La documentación de ProGuard se puede encontrar en <http://developer.android.com/tools/help/proguard.html>
- En iOS se pueden utilizar herramientas similares a ProGuard:
 - iOS Class Guard: <https://github.com/Polidea/ios-class-guard>
 - LLVM obfuscator: <https://github.com/obfuscator-llvm/obfuscator>

◆◆◇ Protección de la aplicación

Destrucción de símbolos del binario

- La destrucción de símbolos del binario (o *binary stripping*) elimina la tabla de símbolos del binario.
- La tabla de símbolos es una estructura de datos creada por el compilador para identificar los nombres de las variables y métodos utilizados en el binario. Su eliminación dificulta la lectura y comprensión del código durante su depuración y análisis estático.
- En Android se puede:
 - Utilizar un compresor de ejecutables como UPX (<http://upx.sourceforge.net>).
 - Utilizar utilidades de consola como `sstrip`.
- En iOS se puede configurar en las opciones del proyecto bajo la pestaña *Build Settings*.

► Deployment Postprocessing	Yes ⇅
Strip Debug Symbols During Copy	Yes ⇅
Strip Linked Product	Yes ⇅
Strip Style	All Symbols ⇅

◆◆◇ Protección de la aplicación

Integridad de la aplicación

- El *repackaging* puede ser utilizado, además de para ataques de ingeniería inversa, para la inyección de código malicioso.
- La aplicación puede verificar la integridad de los componentes de la misma mediante resúmenes o firmas digitales de los distintos componentes de la misma.
- Si se detecta una modificación de la aplicación se puede notificar al *back-end* o borrar los datos sensibles de la aplicación.
- En Android se puede acceder a la información de la firma actual de la aplicación mediante el `PackageManager`:
 - ```
PackageInfo packageInfo =
context.getPackageManager().getPackageInfo(context.getPackageName(),
PackageManager.GET_SIGNATURES);
```
  - `packageInfo.signatures`
- En iOS se puede verificar la validez del recibo de compra de la aplicación ofrecido por el sistema.
  - <https://developer.apple.com/library/mac/releasenotes/General/ValidateAppStoreReceipt/Introduction.html>
- Estas comprobaciones pueden ser eliminadas mediante las técnicas de *repackaging*.

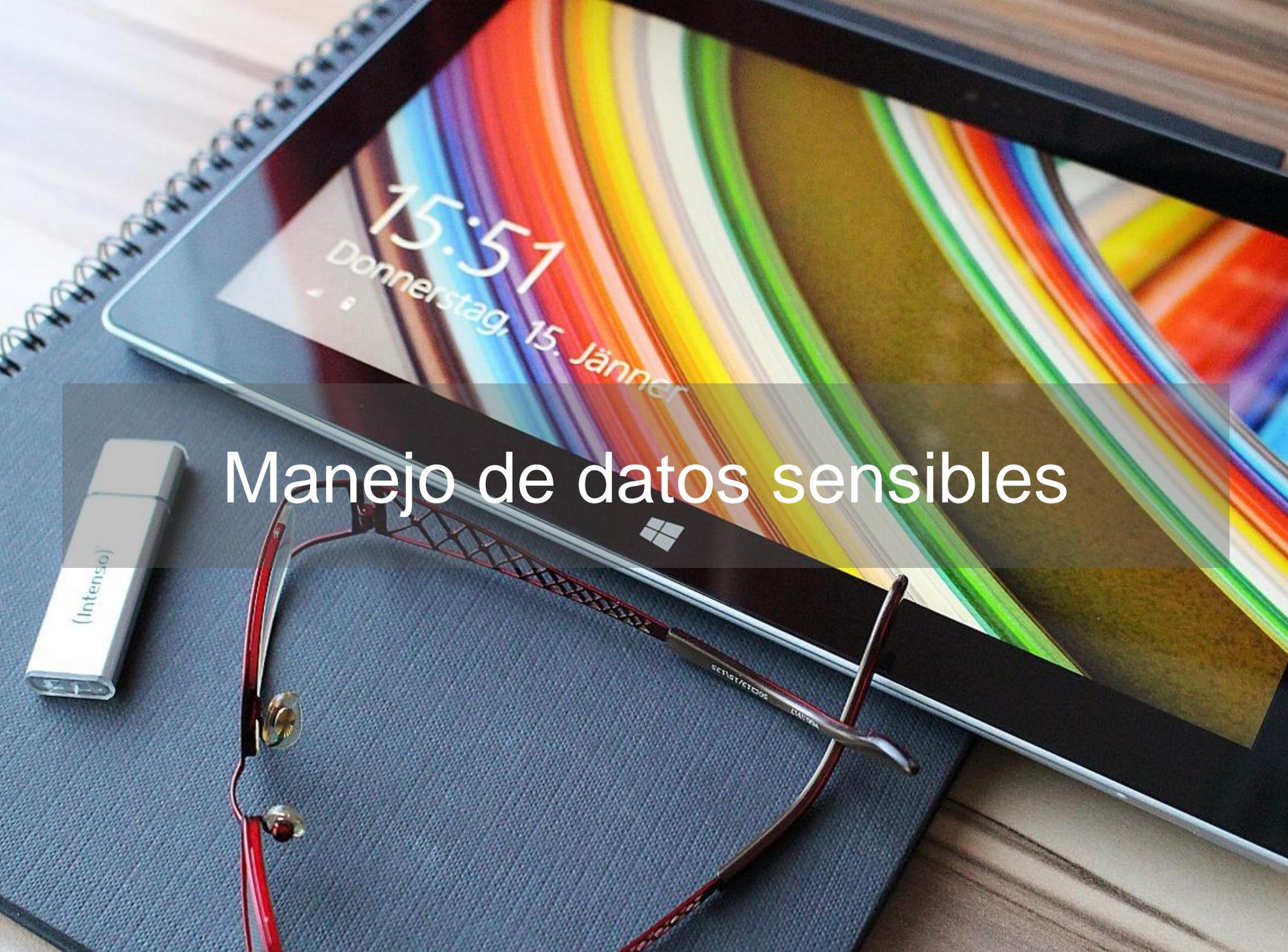
# ◆◆◆ Protección de la aplicación

## Detección de *jailbreak* y *rooting*

- El *jailbreak* o *rooting* de un dispositivo elimina muchas de las medidas de seguridad del sistema para la protección de apps como el *sandboxing*.
- La detección se puede realizar ejecutando alguna de las tareas que sólo se pueden ejecutar en estas condiciones o localizando los ficheros que se instalan durante el proyecto.
- En Android se puede intentar localizar la aplicación supersu o las herramientas busybox:
  - La aplicación supersu tiene nombre de paquete `eu.chainfire.supersu`
  - Ejecutando un comando mediante `Process su = Runtime.getRuntime().exec("comando");`
- En iOS se puede intentar localizar cualquiera de las aplicaciones que se instalan en teléfonos con *jailbreak*.

```
+ (BOOL)isJailbroken{
 if ([[NSFileManager defaultManager] fileExistsAtPath:@"/Applications/Cydia.app"]){
 return YES;
 }else if ([[NSFileManager defaultManager] fileExistsAtPath:@"/Library/MobileSubstrate/MobileSubstrate.dylib"]){
 return YES;
 }else if ([[NSFileManager defaultManager] fileExistsAtPath:@"/bin/bash"]){
 return YES;
 }else if ([[NSFileManager defaultManager] fileExistsAtPath:@"/usr/sbin/sshd"]){
 return YES;
 }else if ([[NSFileManager defaultManager] fileExistsAtPath:@"/etc/apt"]){
 return YES;
 }
 return NO;
}
```

- Este tipo de técnicas se pueden evadir modificando la localización o nombres de los ficheros o a través del *repackaging* de la aplicación.



# Manejo de datos sensibles

# ◆◆◇ Manejo de datos sensibles

## Datos sensibles de una aplicación

- Las aplicaciones móviles manejan datos sensibles de diferente naturaleza durante su ejecución.
- Los diferentes estados en los que se pueden encontrar los datos en un dispositivo son:
  - En reposo: aquellos datos localizados en el almacenamiento persistente del dispositivo como tarjetas de memoria o sistema interno de archivos.
  - En tránsito: los datos que son enviados y recibidos desde el *back-end* y otros dispositivos móviles.
  - En memoria: los datos sobre los que se están ejecutando operaciones y, por lo tanto, se encuentran almacenados en la memoria del dispositivo.
- Para asegurar el correcto tratamiento de los datos durante todo su ciclo de vida se deben seguir una serie de pautas para su tratamiento en cada uno de los estados en los que se puede encontrar.

# ◆◆◇ Manejo de datos sensibles

## Almacenamiento seguro de datos I

- Aquellos datos que se consideren sensibles requieren de una protección específica cuando se encuentran en reposo en el dispositivo.
- La utilización de sistemas de ficheros cifrados limita el acceso de un atacante externo al dispositivo si este se encuentra apagado, pero no evita que otras aplicaciones o procesos del dispositivo puedan realizar lecturas de los datos a través del sistema de ficheros (si los correspondientes permisos lo permiten).
- Para evitar el acceso por parte de terceros se debe evitar la utilización del almacenamiento externo del dispositivo (tarjetas SD, etc.) para el almacenamiento de información sensible.
- En Android se debe evitar el uso del atributo `android:installLocation` que permite que los usuario utilicen el almacenamiento externo para instalar la aplicación.

# ◆◆◇ Manejo de datos sensibles

## Almacenamiento seguro de datos - Android

- Para datos sensibles almacenados en la memoria interna, es recomendable además implementar una capa adicional de cifrado.
- Android no incluye librerías específicas para el cifrado de archivos en reposo (salvo certificados y claves). Para implementar este tipo de cifrado existen dos opciones:
  - Crear desde cero utilizando las librerías de cifrado estándar existentes en la API de Java.
  - Utilizar alguna librería para el almacenamiento seguro de datos como sqlcipher (<http://sqlcipher.net>).
- Para el almacenamiento de claves se pueden utilizar dos API diferentes:
  - KeyChain API para almacenar credenciales que vayan a ser utilizadas a lo largo de todo el sistema (Ej.: certificado raíz de una CA).
  - Keystore para almacenar claves que vayan a ser utilizadas por la aplicación. Desde Android 6.0 es capaz de almacenar claves de cifrado simétricas.

# ◆◆◆ Manejo de datos sensibles

## Almacenamiento seguro de datos - KeyStore

- Las claves generadas mediante el KeyStore incorporan dos medidas de seguridad:
  - Ninguna aplicación tiene acceso directo a las claves. La API del KeyStore se encarga de todas las operaciones.
  - En aquellos dispositivos que cuenten con un entorno de ejecución seguro o un “elemento seguro” (SE), la clave es almacenada dentro del propio SE. En este caso, las aplicaciones le piden al SE que realice las operaciones criptográficas. Las aplicaciones sólo podrán utilizar el SE para aquellas opciones criptográficas para las que el SE es compatible (algoritmos de cifrado, firma, verificación, etc.).
- Además, cada clave almacenada en el KeyStore puede configurarse de tal forma que sólo pueda utilizarse si el usuario ha desbloqueado el teléfono mediante el un patrón, PIN, contraseña o elemento biométrico (desde Android 6.0).



# ◆◆◇ Manejo de datos sensibles

## Almacenamiento seguro de datos – iOS

- En iOS, los datos pueden ser cifrados con una capa adicional de cifrado mediante la utilización de la Data Protection API.
- Cada vez que se crea un fichero mediante `NSFileManager` en iOS se pueden especificar cuatro clases diferentes de protección:
  - `NSFileProtectionComplete`: el fichero se cifrará con una clave derivada del código de bloqueo. La clave solo es accesible con el dispositivo desbloqueado y se descarta 10 segundos después del bloqueo.
  - `NSFileProtectionCompleteUnlessOpen`: la misma protección que en el caso anterior pero si el fichero está abierto mientras el dispositivo se bloquea, la clave no se descarta hasta que el fichero es cerrado.
  - `NSFileProtectionCompleteUntilFirstUserAuthentication`: la clave de cifrado se obtiene tras la primera autenticación y no se olvida hasta que el dispositivo es apagado.
  - `NSFileProtectionNone`: no ofrece ninguna protección adicional.

# ◆◆◇ Manejo de datos sensibles

## Almacenamiento seguro de datos - iOS

- Además, iOS ofrece el Keychain, un contenedor cifrado (también con una clave derivada del código de bloqueo) para el almacenamiento de credenciales por parte de las aplicaciones.
- Los elementos añadidos al Keychain incluyen una serie de atributos que especifican su tipo (usuario, contraseña, certificado, etc.), tipo de autenticación para la que pueden ser utilizados y condiciones para su acceso.
- Además de las condiciones descritas para los ficheros, se añaden nuevas:
  - `kSecAttrAccessibleAfterFirstUnlockThisDeviceOnly`
  - `kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly`
  - `kSecAttrAccessibleAlwaysThisDeviceOnly`
  - `kSecAttrAccessibleWhenUnlockedThisDeviceOnly`
- Que tienen por objetivo evitar la replicación de los elementos introducidos a otros dispositivos que compartan la misma cuenta de iCloud (y tengan el Keychain en la nube activado).

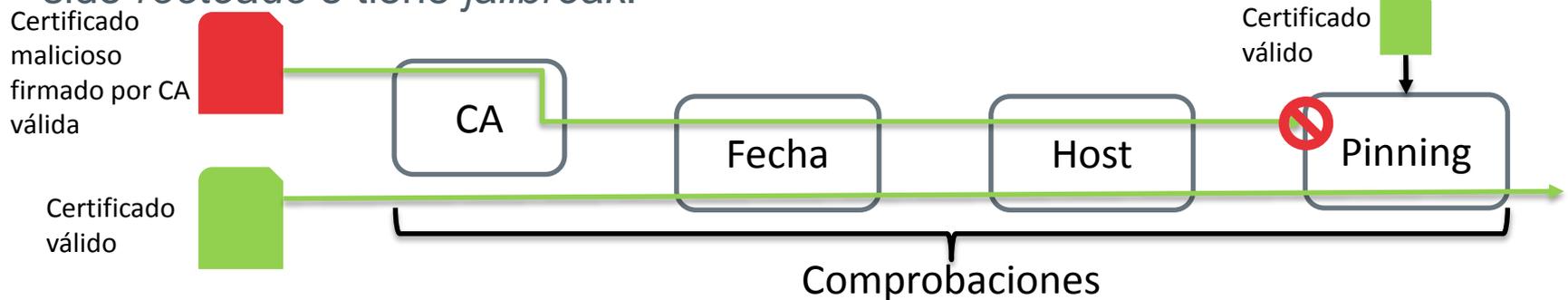
## Seguridad en el transporte de datos – SSL

- Todas las conexiones que incluyan algún tipo de información sensible deberían ser realizadas a través de conexiones SSL que hayan sido completamente validadas.
- Para ello, durante el establecimiento de la conexión hay que verificar una serie de propiedades del certificado:
  - El certificado ha debido ser firmado por una autoridad de certificación válida. Se puede considerar como autoridades válidas aquellas que ya estén en la lista de autoridades válidas del dispositivo o la propia aplicación puede establecer una autoridad válida para sus conexiones (mediante la inclusión del certificado de CA correspondiente).
  - El certificado no debe haber caducado ni debe estar incluido en una lista negra de certificados.
    - Android mantiene una lista negra de certificados no seguros que puede ser actualizada de forma remota.
    - En iOS esa lista se pone al día con las actualizaciones del sistema operativo.
  - El nombre del servidor del certificado debe coincidir con el solicitado.

# ◆◆◇ Manejo de datos sensibles

## Seguridad en el transporte de datos – *Pinning*

- El *certificate pinning* es una técnica que aprovecha que una aplicación móvil se conecta de forma general a un número limitado de servidores.
- Además de las comprobaciones anteriores la aplicación comprobará que el certificado ofrecido por el servidor corresponde a un certificado que la aplicación conoce previamente.
- Las autoridades de certificación comprometidas no afectan a la seguridad de la aplicación. Si se implementa *pinning*, no es necesaria la firma de una CA confiable.
- El pinning puede desactivarse a través de la *repackaging* o si el dispositivo ha sido *rootado* o tiene *jailbreak*.



## ◆◆◆ Manejo de datos sensibles

### Seguridad en el transporte de datos – *Pinning* en Android

- Android permite la implementación de *Certificate Pinning* mediante la definición de un `TrustManager` específico.
- Para ello se debe incorporar el certificado de la CA entre los recursos de la aplicación.

```
// Se crea un KeyStore que contenga el certificado de nuestra CA
Certificate ca = //se lee el certificado de un fichero
keyStoreType = KeyStore.getDefaultType();
KeyStore keyStore = KeyStore.getInstance(keyStoreType);
keyStore.load(null, null);
keyStore.setCertificateEntry("ca", ca);
// Se crea un TrustManager que confie solo en nuestra CA
String tmfAlgorithm = TrustManagerFactory.getDefaultAlgorithm();
TrustManagerFactory tmf = TrustManagerFactory.getInstance(tmfAlgorithm);
tmf.init(keyStore);
// Se crea un contexto (que se utilizará para crear la HttpURLConnection) que incluya nuestro
TrustManager
Context context = SSLContext.getInstance("TLS");
context.init(null, tmf.getTrustManagers(), null
```

## ◆◆◆ Manejo de datos sensibles

### Seguridad en el transporte de datos – *Pinning* en iOS

- En iOS, el pinning se realiza a través del delegado de `NSURLConnection` que incluye el método `willSendRequestForAuthenticationChallenge`.

```
...
SecTrustRef serverTrust = challenge.protectionSpace.serverTrust;
SecCertificateRef certificate = SecTrustGetCertificateAtIndex(serverTrust, 0);
NSData *remoteCertificateData = CFBridgingRelease(SecCertificateCopyData(certificate));
NSData *localCertData = [NSData dataWithContentsOfFile:[NSBundle mainBundle]
pathForResource:@"nombre_fichero" ofType:@"cer"];
if ([remoteCertificateData isEqualToData:localCertData]) {
 NSURLCredential *credential = [NSURLCredential credentialForTrust:serverTrust];
 [[challenge sender] useCredential:credential forAuthenticationChallenge:challenge];
}else {
 // MENSAJE DE ERROR
 [[challenge sender] cancelAuthenticationChallenge:challenge];
}
```

- También se puede implementar mediante la librería [TrustKit](#).

## Variables en memoria



- Cuando el contenido de una variable que contenga información sensible (claves, *tokens* de autenticación, *cookies*, etc.) deje de ser necesario su contenido debe eliminarse de la memoria.
- Es recomendable que este tipo de valores se guarden en arrays de bytes en vez de en objetos como *Strings*.
  - La reasignación de un objeto tipo *String* suele reservar un nuevo espacio de memoria para la nueva referencia pero no elimina la antigua hasta que pasa el recolector de basura.
  - La utilización de un *array* de bytes permite sobre escribir el contenido de la variable en cualquier momento.

# ◆◆◆ Manejo de datos sensibles

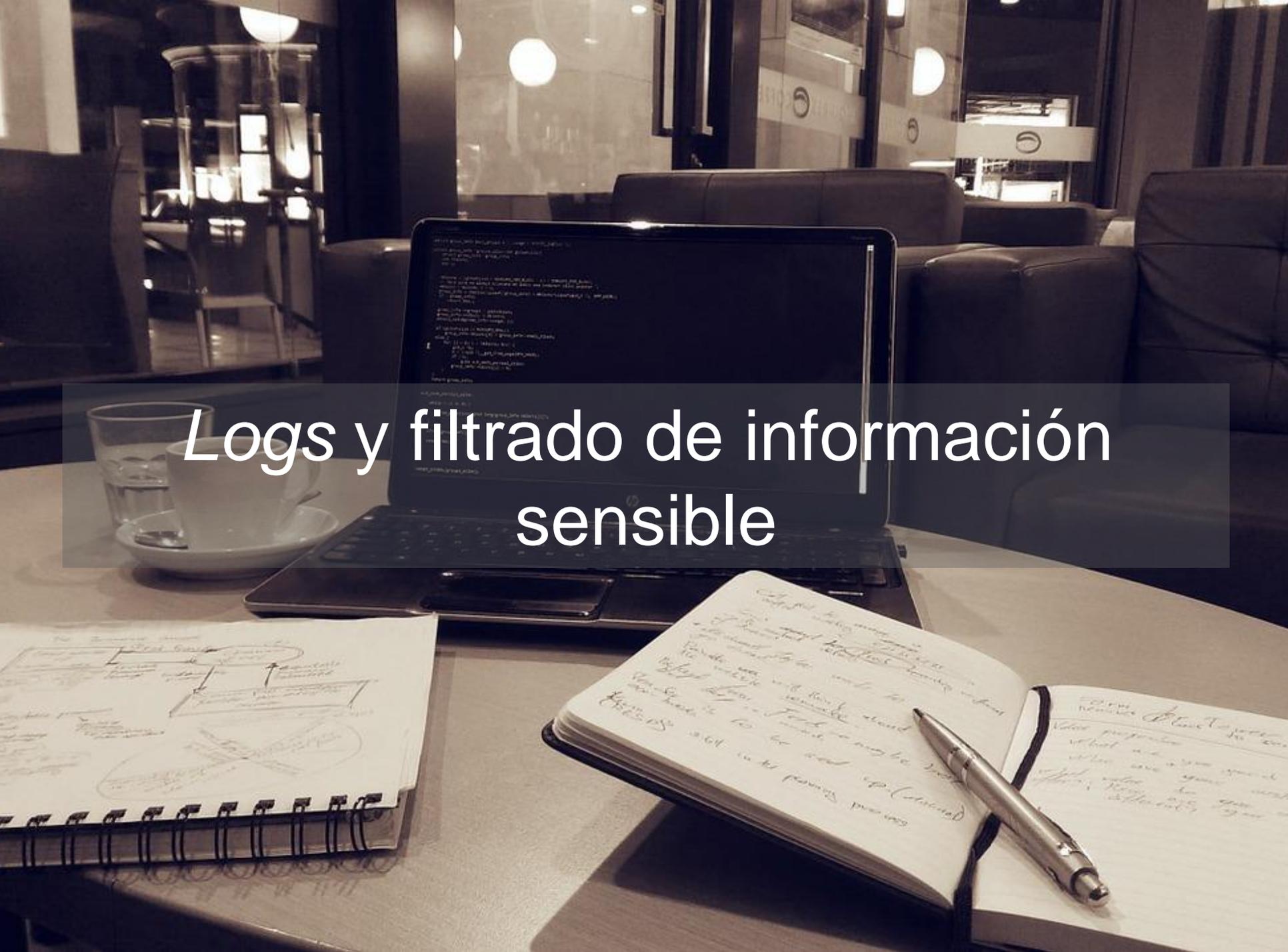
## Cachés

- Siempre que sea posible hay que evitar almacenar datos sensibles en cachés, incluidos:
  - *Cookies*.
  - Ficheros.
  - Bases de datos SQLite.
  - Caché de sitios web.
  - En iOS se puede limitar el caché de sitios web devolviendo `null` en el método

```
willCacheResponse: (NSCachedURLResponse *)connection: (NSURLConnection *)connection
willCacheResponse: (NSCachedURLResponse *)cachedResponse {
 return nil;
}
```

- En Android se puede desactivar la caché para conexiones HTTP mediante el método

```
setUseCaches(boolean) URLConnection connection = miURL.openConnection();
connection.setUseCaches(false);
```

A photograph of a workspace in a cafe. A laptop is open on a table, displaying lines of code on its screen. To the left of the laptop is a white coffee cup on a saucer with a glass of water. In the foreground, there are two spiral-bound notebooks. The notebook on the left contains a hand-drawn diagram with arrows and text. The notebook on the right is open to a page with handwritten notes and a silver pen lies on it. The background shows a dimly lit cafe with leather seating and large windows.

# Logs y filtrado de información sensible

## ◆◆◆ Logs y filtrado de información sensible

### Eliminación de *logs*

- Siempre que sea posible es recomendable eliminar la mayor cantidad posible de logs que genera la aplicación en el dispositivo.
- En Android se puede configurar ProGuard para eliminar los *logs* añadiendo a su fichero de configuración `proguard.cfg`.

```
-assumenosideeffects class android.util.Log {
 > public static *** d(...);
 > public static *** v(...);
 > public static *** i(...);
 > public static *** e(...);
}
```

- En iOS se puede utilizar un macro que en los versiones del desarrollo en producción elimine la sentencia de *log*.

```
#define NSLog(s,...)
```

# ◆◆◇ Logs y filtrado de información sensible

## Caché de teclado

- Se debe evitar que el sistema operativo guarde en su caché de teclado datos sensibles tecleados por el usuario.
- Para las contraseñas se deben utilizar los campos específicos de contraseñas. La información tecleada en estos campos no es guardada en la caché del teléfono.
- Para el resto de campos que puedan almacenar datos sensibles se debe desactivar la opción que guarda los datos tecleados en la caché.
- En Android la única manera consistente de realizar esta operación y que funcione en todos los dispositivos es definir el campo como un campo de contraseña con texto visible. Esto se consigue mediante el atributo `android:inputType="textVisiblePassword"` del campo de texto.
- En iOS se consigue configurando la propiedad `autocorrectionType` del `UITextField` con el valor `UITextAutocorrectionTypeNo`.

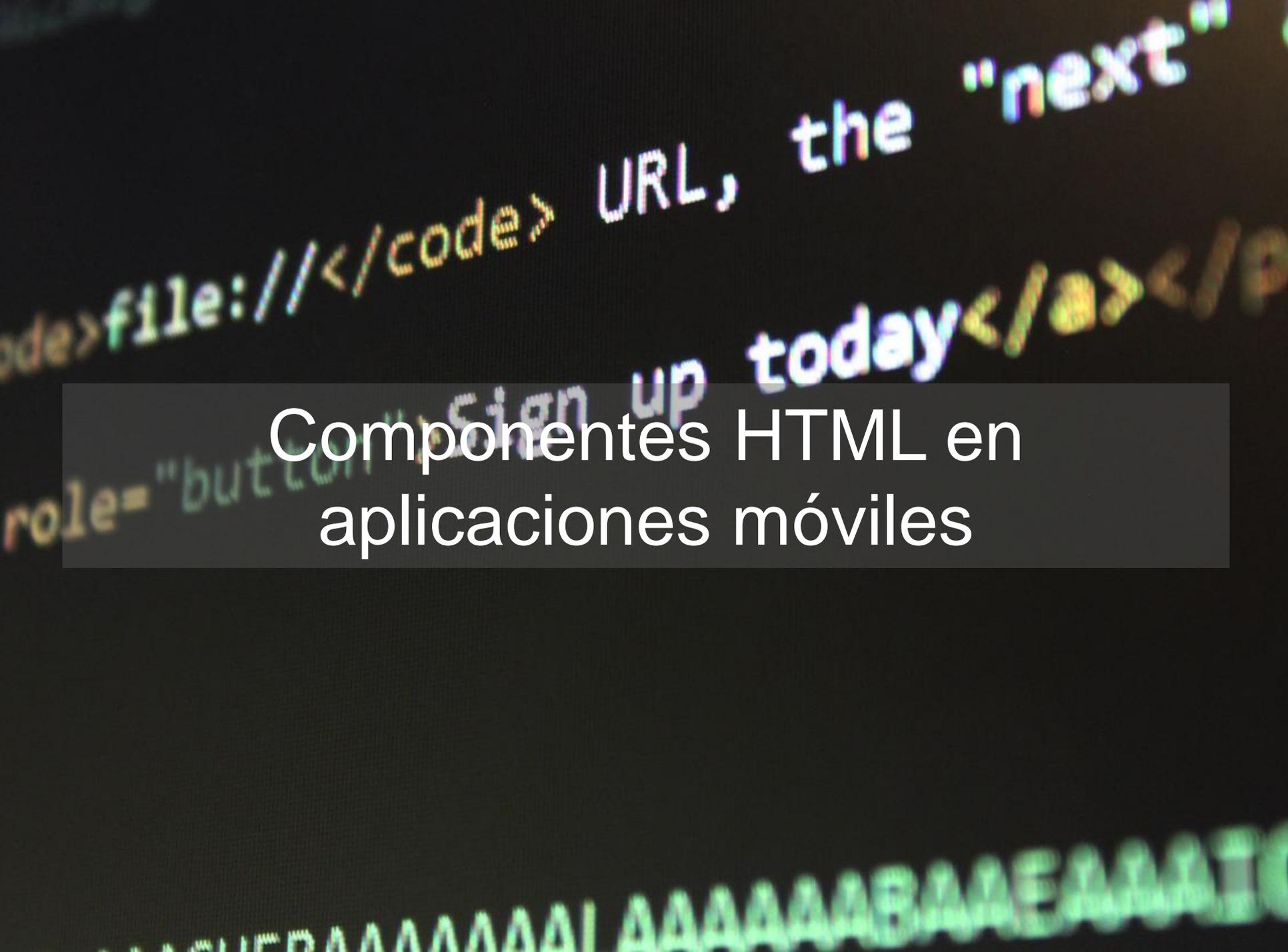
# ◆◆◆ Logs y filtrado de información sensible

## Portapapeles

- Otras aplicaciones pueden acceder a la información almacenada en el portapapeles del sistema sin necesidad de ningún permiso especial.
- En Android se debe crear una subclase de la clase `EditText` y reimplementar los métodos `isSuggestionsEnabled` y `canPaste` para que devuelvan `false`.
- En iOS existen dos opciones:
  - Mediante la creación de una subclase de `UITextField` que no permita las acciones de *copy* o *cut*.

```
-(BOOL)canPerformAction:(SEL)action withSender:(id)sender {
 if (action == @selector(copy:) || action == @selector(cut:)) {
 return NO;
 }
 [super canPerformAction:action withSender:sender];
}
```

- Cuando las funciones `copy` y `cut` se ejecuten, se llama al método `pasteboardWithUniqueName` para obtener el portapapeles específico de la aplicación.



# Componentes HTML en aplicaciones móviles

# ◆◆◇ Componentes HTML en aplicaciones móviles

## Introducción

- Todos los sistemas operativos móviles permiten a las aplicaciones mostrar contenido HTML a través de vistas web.
- La utilización de estas vistas conlleva ciertos riesgos de seguridad que hay que tener en cuenta durante su utilización.
- Para reducir la superficie de ataque generada por estas vistas, se recomienda, independientemente de la plataforma:
  - No cargar nunca contenido remoto mediante conexiones sin cifrar (Sin SSL).
  - Asegurarse de que se utiliza una configuración segura de cifrado SSL y se valida completamente el certificado SSL ofrecido por el servidor.
  - Prohibir el acceso al sistema de ficheros del dispositivo desde la vista web.
  - Desactivar Javascript y cualquier otro *plugin* siempre que sea posible.
  - Verificar que la vista web solo carga URL de los dominios que necesita.
  - No exponer métodos nativos a través de Javascript.
  - No permitir la carga de URL a través de los mecanismos de comunicación con otras aplicaciones.

# ◆◆◆ Componentes HTML en aplicaciones móviles

## Asegurando componentes en Android

- Desactivar Javascript.

```
WebView webview = new WebView(this);
webview.getSettings().setJavaScriptEnabled(false);
```

- Desactivar el acceso al sistema de ficheros.

```
WebView webview = new WebView(this);
webview.getSettings().setAllowFileAccess(false);
```

- Verificar las URL que se cargan en la vista web (extensión de WebView).

```
private class MiWebViewClient extends WebViewClient {
 @Override
 public boolean shouldOverrideUrlLoading(WebView view, String url) {
 //COMPROBACIONES PARA LA URL INICIAL
 }
 @Override
 public WebResourceResponse shouldInterceptRequest(final WebView view, String url){
 //COMPROBACIONES PARA TODAS LAS PETICIONES
 }
}
```

# ◆◆◇ Componentes HTML en aplicaciones móviles

## Asegurando componentes en Android

- Para evitar la carga de URL desde elementos externos a la aplicación se deben eliminar del `manifest` todos los atributos de *exported* de las actividades definidas en la aplicación que tengan una vista web como vista principal.
- La eliminación de los datos de la caché de la vista web se debería realizar una vez se ha dejado de utilizar (método `onPause()` de la actividad).

```
@Override
protected void onPause() {
 ...
 webView.clearCache();
 ...
 super.onPause();
}
```

- Finalmente, se debe evitar exponer el código nativo a la vista utilizando el método `addJavaScriptInterface()`.

# ◆◆◇ Componentes HTML en aplicaciones móviles

## iOS - UIWebView

- Desde iOS 9 , se disponen de tres tipos de vista web.
- UIWebView su uso no está recomendado desde iOS8 pero se puede utilizar en las aplicaciones.
- Utiliza un motor de renderizado no optimizado, por lo que las páginas cargan más lentamente.
- Solo permite la configuración a través de los métodos del delegado, de los cuales el único relevante `webViewShouldStartLoadWithRequest`, que permite identificar la URL a la que se va a conectar la vista web.

```
- (BOOL)webView:(UIWebView*)webView shouldStartLoadWithRequest:(NSURLRequest*)request
navigationType:(UIWebViewNavigationType)navigationType {
 NSURL *url = request.URL;
 //COMPROBACIONES
 return ...;
}
```

- Las vistas web de este tipo no permiten desactivar el motor de Javascript.

# ◆◆◇ Componentes HTML en aplicaciones móviles

## iOS - WKWebView

- [WKWebView](#) es la vista web por defecto utilizada a partir de iOS 8.
- Durante su inicialización se pueden definir una serie de parámetros a través de un objeto del tipo [WKWebViewConfiguration](#).
- Por ejemplo, para desactivar Javascript en la vista se puede utilizar el siguiente código:

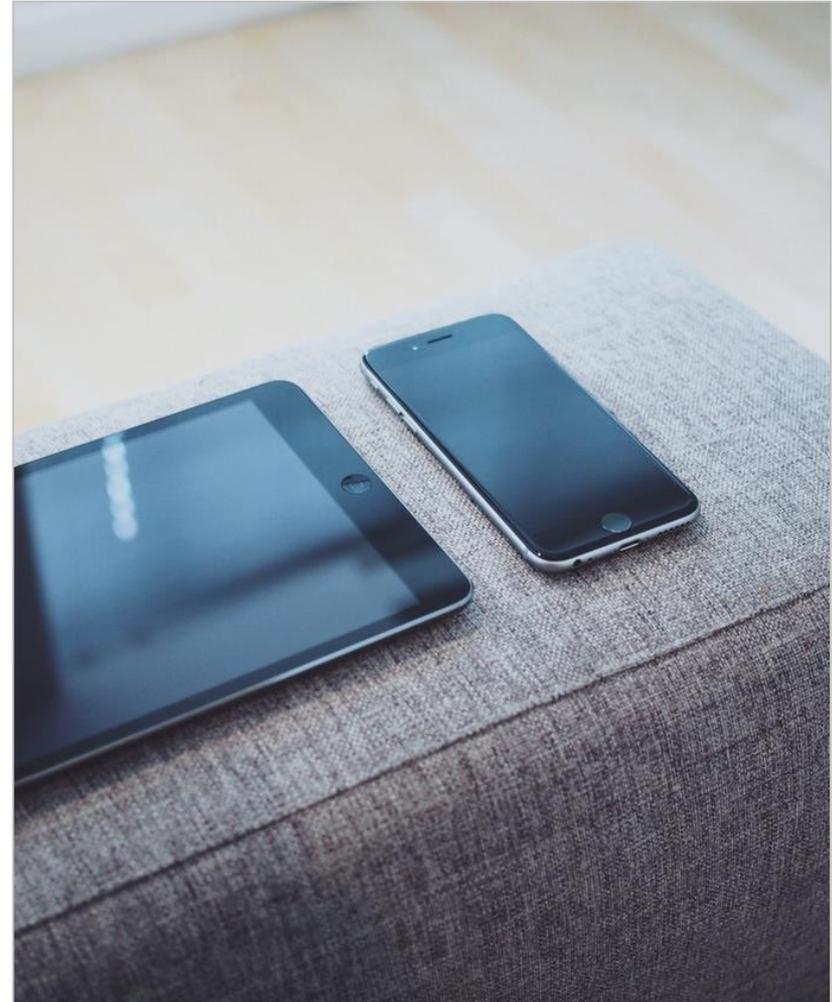
```
WKWebViewConfiguration *conf = [[WKWebViewConfiguration alloc] init];
conf.preferences.javaScriptEnabled = NO
WKWebView *webView = [[WKWebView alloc] initWithFrame:self.view.frame
configuration:conf];
```

- Permite efectuar *certificate pinning* a través del delegado tal y como se mostró anteriormente en la sección de protección de datos sensibles:
  - En iOS 8 existe un error en el delegado, por lo que el *pinning* se debe realizar a revisando los certificados incluidos en la propiedad `certificateChain`.

# ◆◆◇ Componentes HTML en aplicaciones móviles

## iOS - SafariViewController

- SafariViewController ofrece un controlador específico que permite la navegación web desde el interior de la aplicación.
- Este controlador se ejecuta en un proceso diferente a la aplicación que lo invoca.
- El usuario puede acceder a toda la funcionalidad de Safari, incluidos el autorelleno de contraseñas, botón para ejecutar acciones y barra de direcciones en modo lectura.
- La aplicación no puede acceder ni a los sitios que se navegan desde la vista ni a los datos que el usuario introduce en la misma.
- Si la aplicación quiere tener un control mayor sobre el contenido mostrado, deberá utilizar la vista `WKWebView`.





Comunicación entre aplicaciones

# ◆◆◇ Comunicación entre aplicaciones

## Comunicación entre aplicaciones en Android

- La comunicación entre aplicaciones en Android supone un vector adicional de ataque que hay que controlar.
- En primer lugar, todos los elementos de la aplicación que no sirvan específicamente para comunicarse con otras aplicaciones deben ser marcados en el *manifest* con la propiedad `android:exported=false`.

```
<activity android:name=".MyActivity" android:label="Etiqueta"
android:exported=false >
 <intent -filter>
 <action android:name="accion.intent"></action>
 </intent>
</activity>
<service android:enabled="true" android:name=".MyService"
android:exported=false ></service>
<receiver android:enabled="true" android:exported=false
 android:label="My Broadcast Receiver"
 android:name=".MyBroadcastReceiver"
</receiver>
```

# ◆◆◇ Comunicación entre aplicaciones

## Intents

- Se debe evitar enviar información sensible a través de `BroadcastIntents`, ya que actividades maliciosas pueden definir el mismo filtro con mayor prioridad para capturar la información sensible.
- Toda la información recibida de un *Intent* debe ser validada como cualquier otra entrada.
- Se debe evitar definir `IntentFilters` si la actividad no es pública. De esta manera la única manera de acceder a los mismos será a través del nombre de componente.

```
//INTENT CON INFORMACIÓN SENSIBLE: SI ES CAPTURADO LOS DATOS SON COMPROMETIDOS
public static Intent crearIntent(Context context, Usuario user) {
 Intent i = new Intent(context, DetallesUsuario.class);
 i.putExtra(EXTRA_USUARIO, user);
 return i;
}
//INTENT QUE ENVÍA SOLO EL ID DEL USUARIO
public static Intent crearIntent(Context context, String userId) {
 Intent i = new Intent(context, DetallesUsuario.class);
 i.putExtra(EXTRA_USER_ID, userId);
 return i;
}
```

# ◆◆◇ Comunicación entre aplicaciones

## Content Providers

- Los *ContentProviders* ofrecen los datos de la aplicación a aplicaciones de terceros.
- Los *ContentProviders* pueden requerir a otras aplicaciones permisos para leer (`readPermission`), escribir (`writePermission`) o ambos (`permission`) en la base de datos de la aplicación a través del *provider*.

```
<provider android:name="MiProvider"
 android:authorities="com.miapp.provider.MisDatos"
 android:readPermission="permiso.de.lectura"
 android:writePermission="permise.de.escritura"
 android:permission="permiso.para.ambos">
</provider>
```

- Los permisos definidos en el interior del *provider* deben haber sido declarado antes en la aplicación a través de elementos de tipo `<permission>`.
- Un *provider* debe validar todas las peticiones que reciba para evitar inyección de código SQL o acceso a ficheros no autorizados.
- Mediante el atributo `android:grantUriPermissions="true"`. Una aplicación también puede ofrecer acceso esporádico a elementos del *ContentProvider* a aplicaciones que lo soliciten, aunque no hayan definido ningún permiso específico.

# ◆◆◇ Comunicación entre aplicaciones

## Servicios

- Los servicios también pueden exponer funcionalidades o información sensible a aplicaciones de terceros que deben ser protegidos convenientemente.
- Un servicio puede validar método a método los permisos que tiene una aplicación para acceder a una funcionalidad específica a través del método [checkPermission\(\)](#) del PackageManager.
- También se pueden definir los permisos necesarios para comunicarse con el servicio a través del *manifest* de la aplicación.

```
<permission android:name="com.mipermisio" android:label="mi_permiso"
android:protectionLevel="dangerous"></permission>`
<service android:name="com.MiServicio" android:permission="com.mipermisio">
 <intent-filter>
 <action android:name="com.MI_ACCION"/>
 </intent-filter>
</service>
```

# Autenticación en aplicaciones móviles



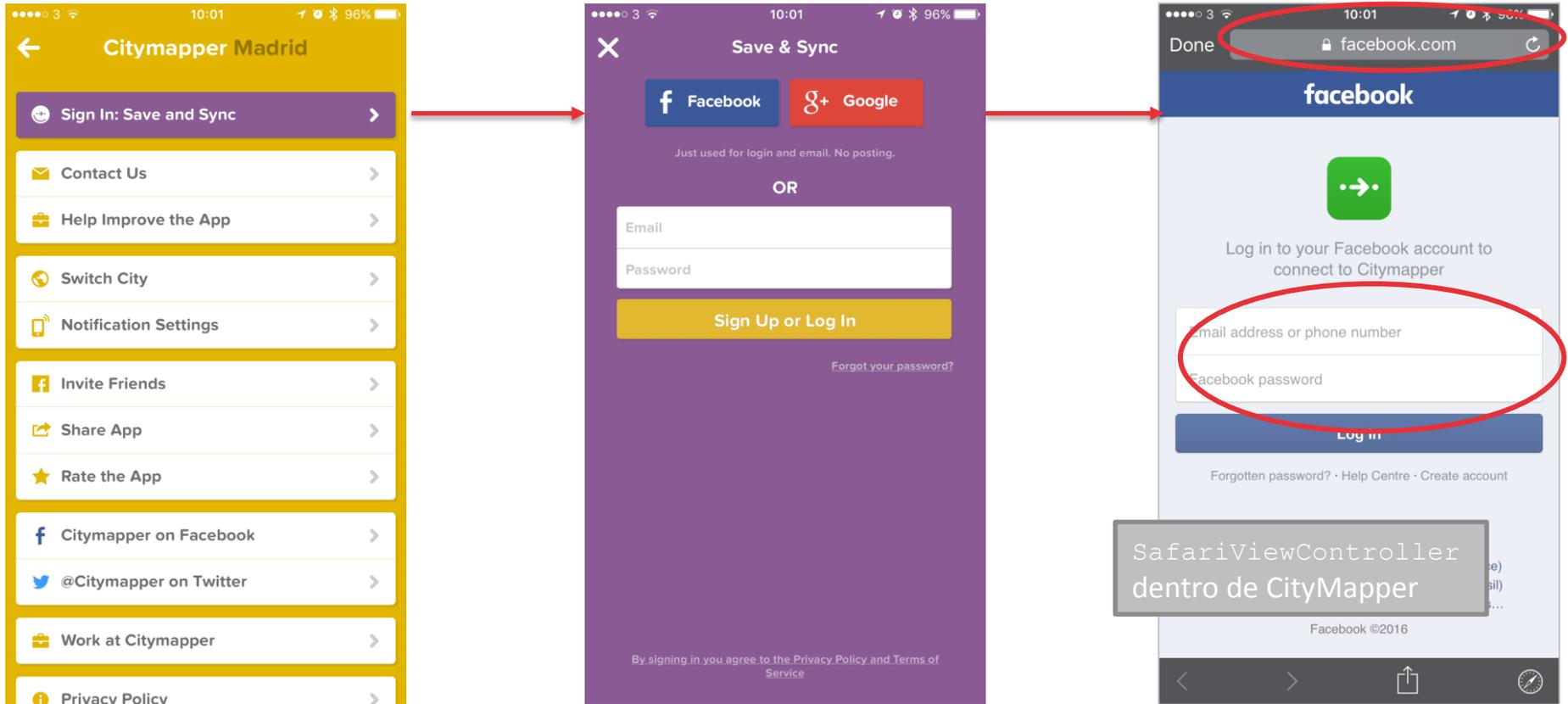
# ◆◆◇ Autenticación en aplicaciones móviles

## Introducción a OAuth

- OAuth es un estándar para la autorización de acceso a recursos/servicios a través de la web.
- Desde el punto de vista del usuario final, OAuth ofrece las siguientes ventajas:
  - Utilización de una sola cuenta para acceder a múltiples servicios.
  - Es necesario recordar menos contraseñas.
  - No es necesario compartir las credenciales (usuario y contraseña generalmente) con un servicio externo en el que no se confía.
  - Se pueden revocar autorizaciones otorgadas de forma sencilla.
- Desde el punto de vista del desarrollador, ofrece las siguientes ventajas:
  - Se simplifica el manejo y cantidad de información sensible a almacenar.
  - No se requiere de un sistema de gestión o renovación de contraseñas.
  - Su implementación se lleva a cabo mediante librerías ampliamente testadas.
  - Existen multitud de proveedores de identidad y otros servicios que ya utilizan OAuth.

# ◆◆◆ Autenticación en aplicaciones móviles

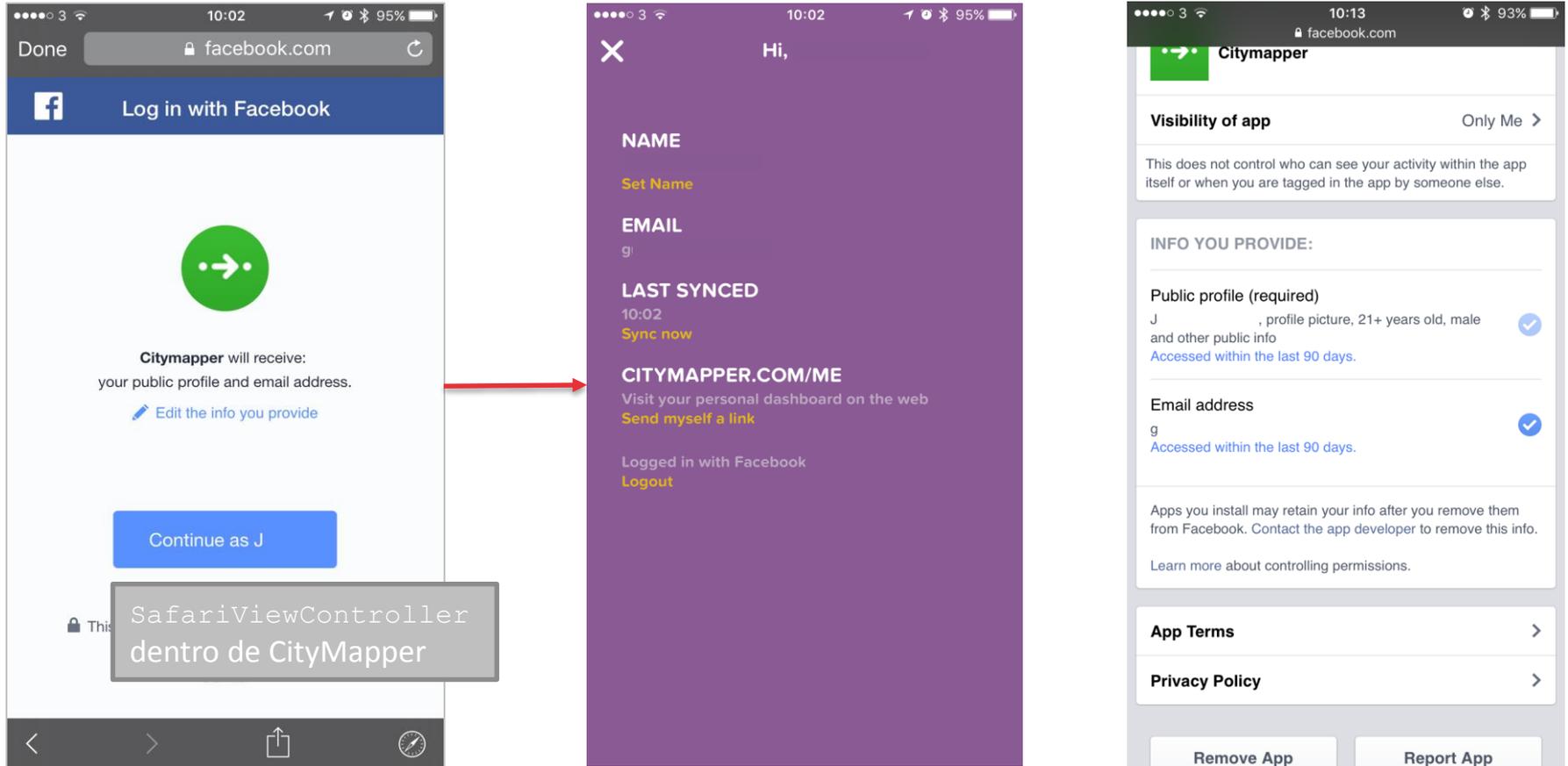
## Con OAuth



Las credenciales sólo se envían al proveedor de la autorización

# ◆◆◆ Autenticación en aplicaciones móviles

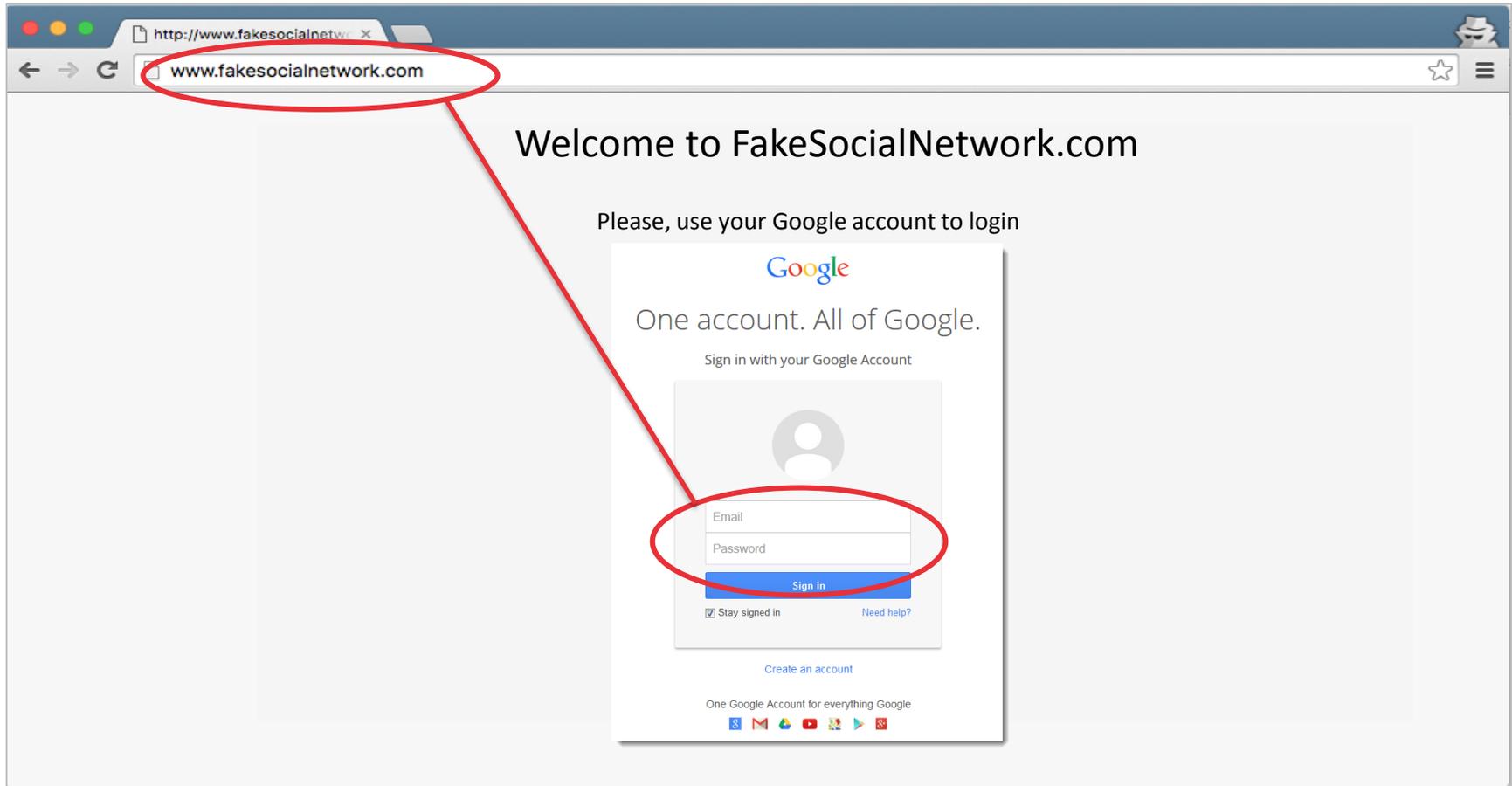
## Con OAuth



El usuario autoriza la información que quiere compartir y en cualquier momento puede modificarla a través del proveedor de la misma

# ◆◆◆ Autenticación en aplicaciones móviles

## La autenticación antes de OAuth

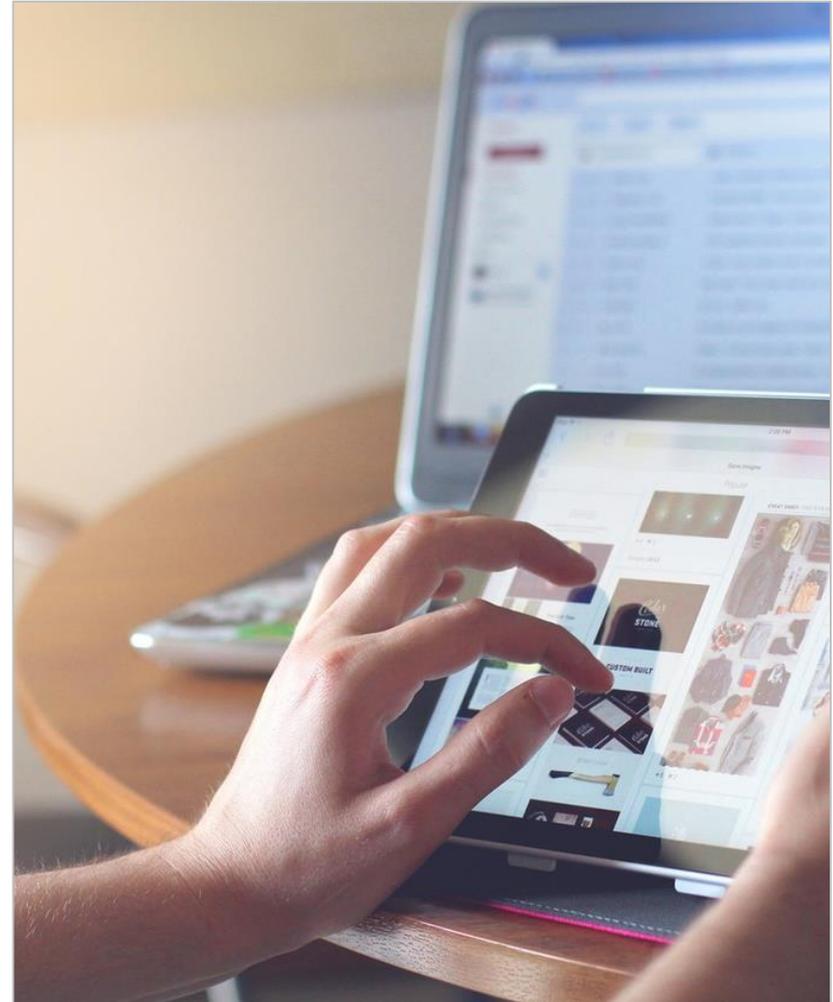


Para autorizar o autenticarnos en una web debíamos introducir las credenciales del proveedor de la autorización en una web no confiable

# ◆◆◆ Autenticación en aplicaciones móviles

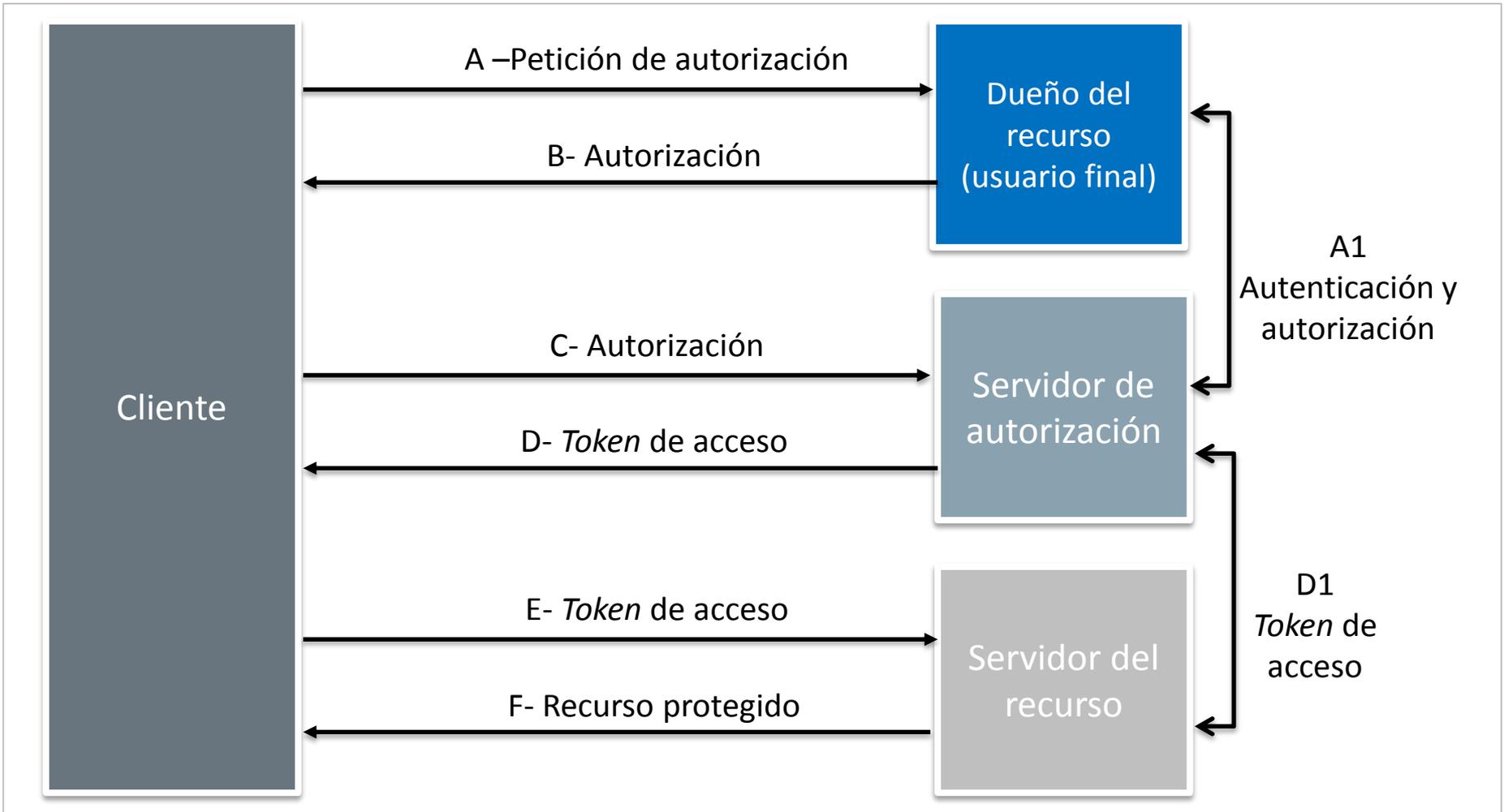
## Roles

- Durante la ejecución del protocolo OAuth participan cuatro roles diferentes:
  - **Dueño el recurso:** es la entidad capaz de autorizar el acceso al recurso en concreto. En la mayoría de los escenarios en el entorno móvil será el usuario final.
  - **Servidor del recurso:** es el servidor que almacena el recurso del cliente. Es capaz de dar acceso al mismo si se le presentan las credenciales oportunas (*tokens* de acceso que se describirán más adelante).
  - **Cliente:** es la aplicación que solicita el acceso al recurso en nombre del dueño del recurso. En el caso de las aplicaciones móviles puede ser la propia aplicación o el *back-end* de la misma.
  - **Servidor de autorización:** es el servidor que genera los *tokens* de acceso para el cliente después de que el dueño del recurso se haya autenticado ante el servidor del recurso. En muchos escenarios los roles de servidor de recursos y servidor de autorización son ejecutados por la misma entidad.



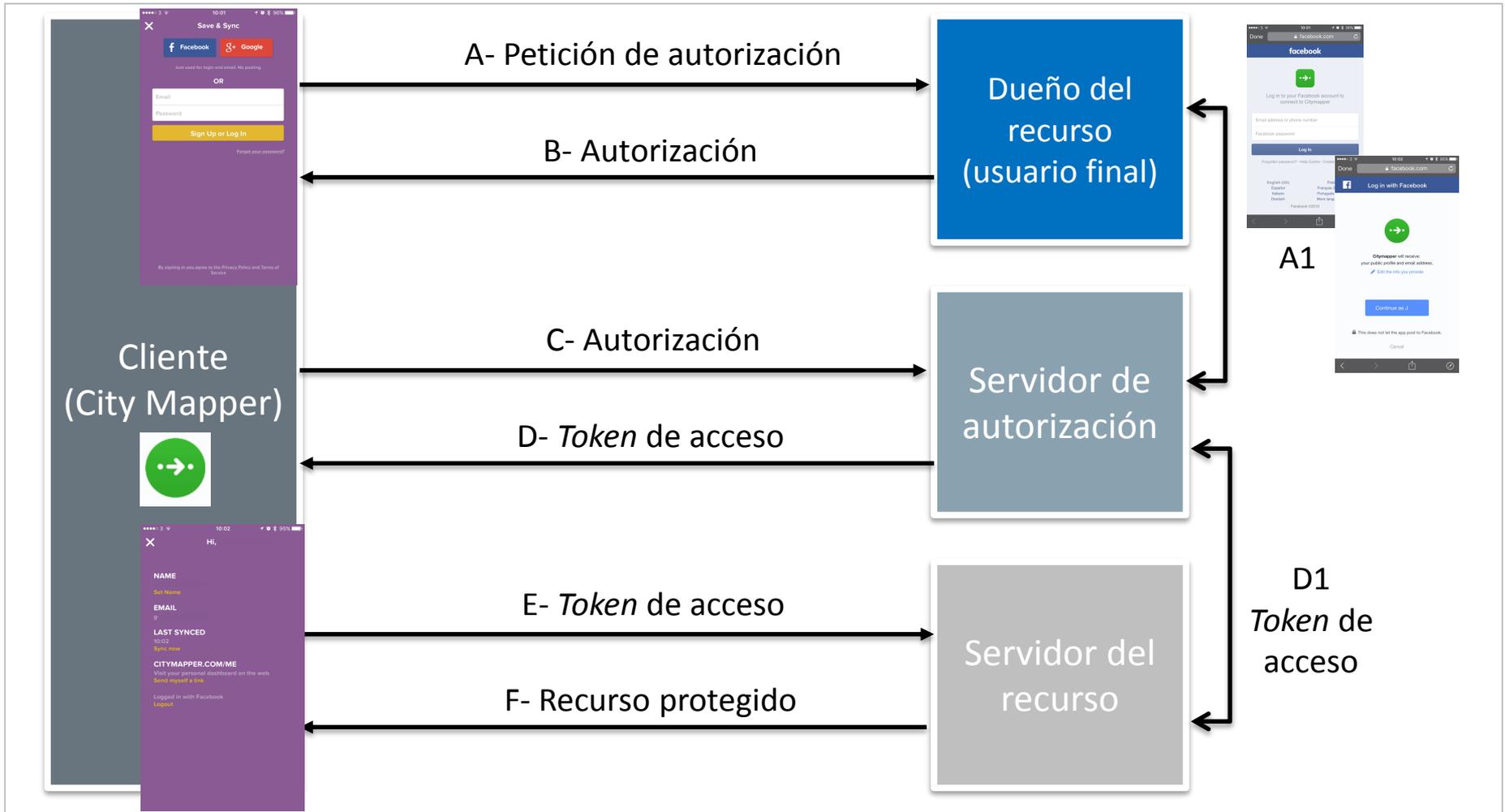
# ◆◆◆ Autenticación en aplicaciones móviles

## Esquema



# Autenticación en aplicaciones móviles

## Esquema en el ejemplo de City Mapper



# ◆◆◇ Autenticación en aplicaciones móviles

## Descripción del esquema

- A) El cliente solicita la autorización del dueño del recurso. La autorización puede ser resuelta de forma local (en el dispositivo móvil) si el recurso (cuenta) está configurado dentro del propio dispositivo (*frameworks* de gestión de cuentas). Si la cuenta no está configurada, se puede obtener con el servidor de autorización como intermediario (A1).
- B) El cliente recibe la autorización (una credencial que representa que el cliente tiene acceso para ese recurso específico). OAuth 2.0 define cuatro tipos diferentes de autorización:
  - Código de autorización: un código de autorización que se obtiene cuando se ejecuta el paso A1.
  - Código implícito: el cliente recibe el *token* de autenticación directamente después de A1. Siempre que sea posible debe evitarse debido a las implicaciones de seguridad.
  - Contraseña: se utiliza un par de credenciales usuario y contraseña. Elimina toda la seguridad del esquema por lo que debe evitarse siempre.
  - Credenciales de cliente: si el recurso pertenece al mismo cliente o ya ha sido permitido su acceso basta con utilizar las credenciales del cliente.

# ◆◆◇ Autenticación en aplicaciones móviles

## Descripción del esquema

- C) El cliente se autentica ante el servidor de autorización con sus propias credenciales (debe estar dado de alta) y la autorización que reciba en el paso anterior.
- D) El servidor valida las credenciales del cliente y la autorización. Si son correctas genera un *token* de acceso:
  - El servidor de autorización y servidor de recursos comparten el *token* de acceso (en caso de que no sean la misma entidad) a través de un canal fuera de banda.
  - El *token* de acceso puede incluir además de los recursos a los que permite el acceso, el tiempo durante el cual el acceso es permitido por el mismo.
- E) El cliente solicita acceso al recurso al servidor de recursos. Para ello presenta el *token* de acceso obtenido en el anterior paso.
- F) El servidor de recursos valida el *token* de acceso y si la validación es correcta envía el recurso solicitado.

# ◆◆◇ Autenticación en aplicaciones móviles

## Autorización en los sistemas operativos móviles

- En el entorno móvil, el servidor de autorización y recursos puede ser accedido a través de tres mecanismos diferentes:
  - **API de cuentas del sistema operativo:** la aplicación que ofrece los recursos debe haber registrado alguna cuenta en el propio sistema operativo. El cliente realiza la solicitud al sistema de cuentas del sistema, que redirige la solicitud a la API de autenticación/autorización específica de la cuenta seleccionada por el usuario.
  - **Aplicaciones:** es similar al caso anterior, pero el cliente solicita directamente la autorización al servidor de recursos/autorización a través de una aplicación específica ya instalada en el cliente. Para ello se utilizan las librerías de comunicación entre aplicaciones.
  - **Vistas web:** si la aplicación del servidor de recursos/autorización no está instalada en el dispositivo, se puede utilizar una vista web para la realización del proceso. Una vez el usuario se ha autorizado, el cliente puede extraer el *token* de acceso de la vista web correspondiente.

# ◆◆◆ Autenticación en aplicaciones móviles

## Autorización en Android – AccountManager I

- El `AccountManager` de Android se puede utilizar para realizar peticiones de autorización a la cuenta de Google instalada en el dispositivo o a cuentas de otros proveedores que hayan implementado los métodos necesarios dentro de su aplicación.
- Permisos requeridos para acceder a las cuentas del dispositivo.

```
<uses-permission android:name="android.permission.GET_ACCOUNTS" />
<uses-permission android:name="android.permission.INTERNET" />
<uses-permission android:name="android.permission.USE_CREDENTIALS" />
```

- Durante la creación de la actividad se verifica si el usuario ya ha dado su autorización.

```
protected void onCreate(Bundle savedInstanceState) {
 super.onCreate(savedInstanceState);
 AccountManager accountManager = AccountManager.get(this);
 if (tokenGuardado() != null) {
 accionesAutenticado(tokenGuardado());
 } else {
 escogerCuenta();
 }
}
```

# ◆◆◆ Autenticación en aplicaciones móviles

## Autorización en Android – AccountManager II

- Si el cliente no ha sido autorizado se deberá solicitar la cuenta con la que queremos acceder al recurso (com.paquete.cuenta).

```
private void escogerCuenta() {
 int ACCOUNT_REQUEST_CODE = 1601;
 Intent intent = AccountManager.newChooseAccountIntent(null, null,
 new String[] { "com.paquete.cuenta" }, false, null, null, null, null);
 startActivityForResult(intent, ACCOUNT_REQUEST_CODE);
}
```

- La respuesta incluirá el nombre de cuenta, por lo que debemos obtener la cuenta y realizar la petición del *token* de autenticación para ese recurso.

```
protected void onActivityResult(int requestCode, int resultCode, Intent data) {
 super.onActivityResult(requestCode, resultCode, data);
 if (resultCode == RESULT_OK) {
 if (requestCode == ACCOUNT_REQUEST_CODE) {
 String accountName = data.getStringExtra(AccountManager.KEY_ACCOUNT_NAME);
 for (Account account : accountManager.getAccountsByType("com.paquete.cuenta")) {
 if (account.name.equals(accountName)) {
 userAccount = account;
 break;
 }
 }
 //RECURSO DEPENDERÁ DEL RECURSO AL QUE QUERAMOS ACCEDER
 //PARA HANGOUTS SE REQUIERE "https://www.googleapis.com/auth/googletalk";
 accountManager.getAuthToken(userAccount, "oauth2:" + RECURSO, null, this,
 new OnTokenAcquired(), null);
 }
 }
}
```

# ◆◆◆ Autenticación en aplicaciones móviles

## Autorización en Android – AccountManager III

- Una vez obtenido el *token* de autorización se llama a un nuevo objeto de tipo `OnTokenAcquired` que hace de *callback* para la recepción del *token* de autenticación. El *token* debería ser guardado como un dato sensible de la aplicación.

```
private class OnTokenAcquired implements AccountManagerCallback<Bundle> {
 @Override
 public void run(AccountManagerFuture<Bundle> result) {
 try {
 Bundle bundle = result.getResult();
 Intent launch = (Intent) bundle.get(AccountManager.KEY_INTENT);
 if (launch != null) {
 //AUTORIZACION FALLIDA, SE DEBE VOLVER A INTENTAR
 startActivityForResult(launch, AUTHORIZATION_CODE);
 } else {
 String token = bundle.getString(AccountManager.KEY_AUTHTOKEN);
 guardarToken(token)
 accionesAutenticado(token);
 }
 } catch (Exception e) {
 throw new RuntimeException(e);
 }
 }
}
```

# ◆◆◇ Autenticación en aplicaciones móviles

## Autorización en Android – SDKs de aplicaciones

- Es posible que el servidor de recursos acepte peticiones de recursos a través de su propia aplicación, pero sin la integración con el sistema de cuentas de Android.
- En esos casos, el propio servicio suele ofrecer documentación exhaustiva de cómo utilizar la aplicación para la solicitud de *tokens* de autenticación.
- La documentación suele incluir el proceso de registro de la aplicación cliente y como realizar las llamadas entre ambas aplicaciones para solicitar y recibir el *token* de autorización.
- Ejemplos de este tipo de autorización son:
  - Facebook: <https://developers.facebook.com/docs/facebook-login/android>
  - Twitter: a través de las API de:
    - Twitter Kit para Android <https://github.com/twitter/twitter-kit-android>
    - Twitter Core si se utiliza Fabric <https://docs.fabric.io/android/twitter/twitter-core.html>

# ◆◆◆ Autenticación en aplicaciones móviles

## Autorización en Android - Navegador

- Si la aplicación no está instalada se puede hacer uso de una WebView (vista web ofrecida por el sistema) para acceder a la información. El funcionamiento de OAuth puede diferir de un servicio a otro.

```
@Override
public void onCreate(Bundle savedInstanceState) {
 super.onCreate(savedInstanceState);
 setContentView(R.layout.main);
 String url = URL_DE_OAUTH + "?client_id=" + ID_NUESTRA_APP_EN_SERVICIO_OAUTH;
 WebView webview = (WebView)findViewById(R.id.webview);
 webview.getSettings().setJavaScriptEnabled(true);
 webview.setWebViewClient(new WebViewClient() {
 public void onPageStarted(WebView view, String url, Bitmap favicon) {
 String accessTokenFragment = "access_token=";
 String accessCodeFragment = "code=";
 if (url.contains(accessTokenFragment)) {
 // Capturamos las peticiones para buscar los codigos de autorization y el token
 String accessToken = url.substring(url.indexOf(accessTokenFragment));
 guardarToken(accessToken);
 } else if (url.contains(accessCodeFragment)) {
 // Si es un access code realizamos otra peticion para obtener el token
 String accessCode = url.substring(url.indexOf(accessCodeFragment));
 guardarCodigoAutorizacion(accessCode);
 String query = "client_id=" + ID_NUESTRA_APP_EN_SERVICIO_OAUTH + "&client_secret=" +
 SECRETO_OBTENIDO_DURANTE_EL_REGISTRO_DE_NUESTRA_APP+ "&code=" + accessCode;
 view.postUrl(OAUTH_ACCESS_TOKEN_URL, query.getBytes());
 }
 }
 });
 webview.loadUrl(url);
}
```

# ◆◆◆ Autenticación en aplicaciones móviles

## Autorización en iOS - *Accounts Framework*

- iOS permite la configuración de las cuentas de Facebook y Twitter en los ajustes del propio dispositivo, de tal forma que otras aplicaciones pueden solicitar el acceso a los mismos.
- En este caso las preferencias de privacidad de iOS permiten revocar directamente los *tokens* de acceso.
- A continuación se muestra un ejemplo para el acceso a la cuenta de correo almacenada en la cuenta de Facebook del usuario.

```
ACAccountStore *accountStore = [[ACAccountStore alloc] init];
ACAccountType *accountType = [accountStore
ccountTypeWithIdentifier:ACAccountTypeIdentifierFacebook];
NSDictionary *options = @{ ACFacebookAppIdKey : APPID_DEL_CLIENTE_EN_FACEBOOK,
 ACFacebookPermissionsKey : @[@"email"]
 };
[accountStore requestAccessToAccountsWithType:accountType
 options:options
 completion:^(BOOL granted, NSError *error){
 if (granted) {
 _currentUser.facebook = [accounts firstObject];
 } else {
 //MOSTRAR MENSAJE DE ERROR
 }
 }];
```

# ◆◆◆ Autenticación en aplicaciones móviles

## Autorización en iOS – SDKs de aplicaciones

- De la misma manera que en Android, es posible que el servidor de recursos acepte peticiones de recursos a través de su propia aplicación instalada en iOS.
- En esos casos, el propio servicio suele ofrecer documentación exhaustiva de cómo utilizar la aplicación para la solicitud de *tokens* de autenticación.
- Ejemplos de este tipo de autorización son:
  - Facebook:  
<https://developers.facebook.com/docs/facebook-login/ios>
  - Foursquare:  
<https://developer.foursquare.com/resources/libraries>
  - Twitter: a través de la API de Fabric:  
<https://docs.fabric.io/ios/twitter/authentication.html>



# ◆◆◇ Autenticación en aplicaciones móviles

## Autorización en iOS – Vistas web

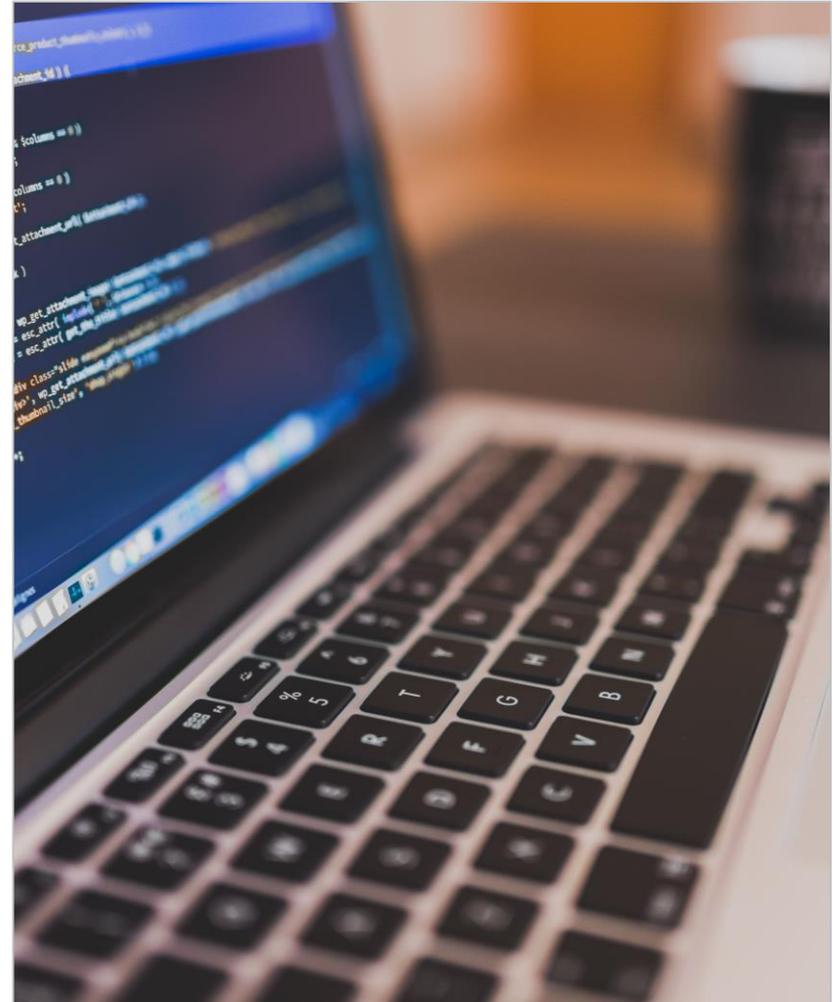
- En iOS se puede utilizar cualquiera de las tres vistas web disponibles para implementar OAuth.
- Tanto UIWebView como WKWebView permiten acceder a las credenciales que el usuario escribe dentro de la vista por lo que se recomienda la utilización de SafariViewController.
- SafariViewController corre en un proceso separado y además, no requerirá al usuario las credenciales si ya se han utilizado previamente con Safari.
- Existe una librería OAuthSwift con soporte para realizar peticiones OAuth a través de SafariViewControllers escrita en Swift.
  - <https://github.com/mwermuth/OAuthSwift/tree/swift2.0>
- Entre los servicios soportados se pueden encontrar Twitter, Flickr, Github, Instagram, Foursquare, Fitbit, LinkedIn, Dropbox y Salesforce entre otros.



# Laboratorio

## Introducción

- Durante esta parte de la unidad vamos a llevar a cabo dos laboratorios para mostrar de forma práctica las directrices y buenas practicas descritas a lo largo de la unidad.
- Los laboratorios van a consistir en solucionar las vulnerabilidades que se identificaron en las dos aplicaciones (Android e iOS) analizadas durante la unidad 3.
- Durante los laboratorios nos vamos a centrar en tareas relacionadas con el código de la aplicación. Un S-SDLC debe expandir sus actividades a lo largo de todas las tareas que componen el desarrollo de la aplicación.



## Tareas

- Los diferentes modificaciones que se realizarán al código fuente de las aplicaciones se han organizado en tareas.
- Las tareas encapsulan un trabajo que debe realizar el alumno por su cuenta.
- Para motivar el aprendizaje, las tareas están divididas en dos partes fundamentales:
  - Motivación y descripción de la tarea que se va realizar, incluyendo, además, el tipo de resultados esperados.
  - Procedimiento para ejecutar la tarea y resultados esperado.
- Ambas partes se describirán separadas en diferentes páginas.
- Con esto se pretende que intentes la realización de la tarea sin tener acceso al procedimiento.
- Más adelante podrás utilizar el procedimiento descrito para verificar tu solución y resolver posibles dudas.

A group of green Android robots standing in a line, with the text "Laboratorio de Android" overlaid in the center.

Laboratorio de Android

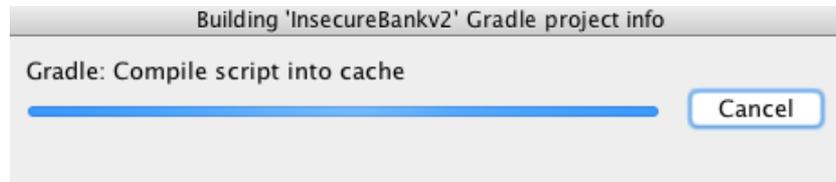
## Procedimiento

<input checked="" type="checkbox"/>	_____

- Las tareas a efectuar durante este laboratorio son las siguientes:
  - Preparación del entorno de trabajo.
  - Configuración correcta de componentes de la aplicación.
  - Almacenamiento de credenciales.
  - Eliminación de funcionalidad de administrador.
  - Eliminación de fugas de información a través de los *logs*.
  - Permisos.

## Preparación del entorno

- Se crea una carpeta en **Santoku** o en el equipo en el que esté instalado el entorno para el desarrollo de Android:
  - > `cd Documents`
  - > `mkdir laboratorio_android`
  - > `de laboratorio_android`
- Se clona el repositorio:
  - > `git clone https://github.com/dineshshetty/Android-InsecureBankv2.git`
  - > `git checkout 6267a02c80a6a5bfff7c26b71d9125c0c7039fe79 .`
  - > `cd Android-InsecureBankv2`
- En Android Studio se navega hasta la carpeta *InsecureBankv2* en el directorio anterior y se selecciona “Choose”.
- Tras un periodo de carga se mostrará la ventana de Android Studio con el proyecto.



### Configuración correcta de componentes de la aplicación

- En esta tarea se van resolver todos los problemas que se detectaron en la configuración de los componentes durante el análisis de la aplicación.

#### **Tarea**

Modifica la configuración de todos los componentes de la aplicación declarados en el *manifest* para que no puedan ser utilizados por otras aplicaciones de forma maliciosa.

#### **Resultado esperado**

Un fichero *manifest* con la configuración de seguridad correcta para cada uno de los componentes de la aplicación.

## Configuración correcta de componentes de la aplicación

### Solución

- En primer lugar se verifican los elementos que tienen *exported=true*.
- Actividades:

```
<activity
 android:name=".ChangePassword"
 android:exported="true"
 android:label="@string/title_activity_change_password" >
</activity>
<activity
 android:name=".DoTransfer"
 android:exported="true"
 android:label="@string/title_activity_do_transfer" >
</activity>
```

```
<activity
 android:name=".ViewStatement"
 android:exported="true"
 android:label="@string/title_activity_view_statement" >
</activity>
<activity
 android:name=".PostLogin"
 android:exported="true"
 android:label="@string/title_activity_post_login" >
</activity>
```

- *Receivers:*

```
<receiver
 android:name=".MyBroadCastReceiver"
 android:exported="true" >
 <intent-filter>
 <action android:name="theBroadcast" >
 </action>
 </intent-filter>
</receiver>
```

- *Provider:*

```
<provider
 android:name=".TrackUserContentProvider"
 android:authorities="com.android.insecurebankv2.TrackUserContentProvider"
 android:exported="true" >
</provider>
```

### Configuración correcta de componentes de la aplicación

#### **Solución**

- Analizando la funcionalidad de las actividades, ninguna de ellas necesita ser accedida por otras aplicaciones por lo que se elimina el atributo.
- Analizando la funcionalidad del receiver se observa, por los comentarios y el código del mismo, que su objetivo es enviar un mensaje SMS con la confirmación del cambio de contraseña al usuario.
- No debería ejecutarse desde el teléfono por diversos motivos:
  - Supone un coste económico para el mismo.
  - Es altamente probable que el usuario ejecute la aplicación en el mismo teléfono en el que ha configurado cuenta bancaria.
  - La operación no se está realizando desde un elemento confiable del sistema (el teléfono).
- Por lo tanto, de momento, se elimina la funcionalidad de la aplicación móvil eliminando la mención al receiver del manifest (además del código).
- La funcionalidad del receiver se debería implementar en el servidor a través de una pasarela SMS (fuera del ámbito de este laboratorio).

## Configuración correcta de componentes de la aplicación

### Solución

- También se debe eliminar el código correspondiente que se encarga de ejecutar el *BroadcastIntent* una vez se ha realizado el cambio de contraseña.
- Este código se encuentra localizado en la Actividad *ChangePassword*.

```
/*
The function that handles the SMS activity
phoneNumber: Phone number to which the confirmation SMS is to be sent
*/

broadcastChangepasswordSMS(phoneNumber, changePassword_text.getText().toString());
```

```
private void broadcastChangepasswordSMS(String phoneNumber, String pass) {

 if(TextUtils.isEmpty(phoneNumber.toString().trim())) {

 System.out.println("Phone number Invalid.");
 }
 else
 {
 Intent smsIntent = new Intent();
 smsIntent.setAction("theBroadcast");
 // String actdngs= smsIntent.getAction().toString();
 // Toast.makeText(getApplicationContext(),actdngs , Toast.LENGTH_LONG).show();
 smsIntent.putExtra("phonenumber", phoneNumber);
 smsIntent.putExtra("newpass", pass);
 sendBroadcast(smsIntent);
 }
}
```

## Configuración correcta de componentes de la aplicación

### Solución

- El *provider* `TrackUserContentProvider`, como su descripción indica, se encarga de mantener un listado de los usuarios registrados en la aplicación.
- Sin entrar a valorar la necesidad de este tipo de *provider* en un entorno real y si la implementación es correcta (se verificará en otra tarea), se va a proteger el mismo mediante la definición de nuevos permisos para mostrar el procedimiento de protección de un *provider* mediante permisos.
- De esta manera las aplicaciones que quieran acceder a esta información deberán declarar alguno de los nuevos permisos.

```
<permission android:name="com.android.insecurebankv2.READ_TRACKING" />
<permission android:name="com.android.insecurebankv2.WRITE_TRACKING" />

<provider
 android:name=".TrackUserContentProvider"
 android:authorities="com.android.insecurebankv2.TrackUserContentProvider"
 android:exported="true"
 android:readPermission="com.android.insecurebankv2.READ_TRACKING"
 android:writePermission="com.android.insecurebankv2.WRITE_TRACKING" >
</provider>
```

- En primer lugar se definen los permisos y a continuación se asignan en el *provider*.

## Almacenamiento de credenciales

- En esta tarea se va a revisar el código relativo al almacenamiento de credenciales que se realiza en la actividad `DoLogin` para adecuar su seguridad.

### **Tarea**

Revisa y toma las acciones oportunas con respecto al almacenamiento de los credenciales que se realiza por defecto en la actividad `DoLogin`.

### **Resultado esperado**

Una actividad `DoLogin` que no almacene los credenciales del usuario de forma insegura.

## Almacenamiento de credenciales

### Solución

- En primer lugar estudiamos el código del método mencionado en el enunciado.

```
/*
The function that saves the credentials locally for future reference
username: username entered by the user
password: password entered by the user
*/
private void saveCreds(String username, String password) throws UnsupportedOperationException, InvalidKeyException {
 // TODO Auto-generated method stub
 SharedPreferences mySharedPreferences;
 mySharedPreferences = getSharedPreferences(MYPREFS, Activity.MODE_PRIVATE);
 SharedPreferences.Editor editor = mySharedPreferences.edit();
 rememberme_username = username;
 rememberme_password = password;
 String base64Username = new String(Base64.encodeToString(rememberme_username.getBytes(), 4));
 CryptoClass crypt = new CryptoClass();
 superSecurePassword = crypt.aesEncryptedString(rememberme_password);
 editor.putString("EncryptedUsername", base64Username);
 editor.putString("superSecurePassword", superSecurePassword);
 editor.commit();
}
```

- Se puede ver que se está utilizando una clase propia para realizar el cifrado de las credenciales y luego se almacenan en un fichero de *SharedPreferences*.
- El análisis de la librería criptográfica propia revela que no se está utilizando la criptografía de forma segura.

```
// The super secret key used by the encryption function
String key = "This is the super secret key 123";

// The initialization vector used by the encryption function
byte[] ivBytes = {
 0x00, 0x00
};
```

## Almacenamiento de credenciales

### Solución

- Dado que los credenciales que se están almacenando son relativos a una cuenta bancaria, los credenciales no deberían ser almacenados en el dispositivo.
- La primera alternativa debería ser por lo tanto la eliminación de la funcionalidad de la aplicación relativa al almacenamiento de estos credenciales.
- Durante la eliminación se comprueba que si el login es correcto los detalles del mismo se muestran en el *log* del dispositivo. Se procede a la eliminación de esa funcionalidad también.

```
InputStream in = responseBody.getEntity().getContent();
result = convertStreamToString(in);
result = result.replace("\n", "");
if (result != null) {
 if (result.indexOf("Correct Credentials") != -1) {
 Log.d("Successful Login:", " account=" + username + ":" + password);
 trackUserLogins();
 Intent pL = new Intent(getApplicationContext(), PostLogin.class);
 pL.putExtra("uname", username);
 startActivity(pL);
 } else {
 Intent xi = new Intent(getApplicationContext(), WrongLogin.class);
 startActivity(xi);
 }
}
}
```



## Almacenamiento de credenciales

### Solución

- Además se procede también a la eliminación de los elementos del interfaz que permiten restablecer las credenciales guardadas y a los métodos que recuperan la información desde la actividad *LoginActivity* y su interfaz correspondiente.
- Botón para el relleno de datos:

```
Button fillData_button;
```

- Inicialización desde `onCreate()`:

```
fillData_button = (Button) findViewById(R.id.fill_data);
fillData_button.setOnClickListener((v) -> {
 // TODO Auto-generated method stub
 try {
 fillData();
 } catch (InvalidKeyException | UnsupportedEncodingException e) {
 // TODO Auto-generated catch block
 e.printStackTrace();
 }
});
```

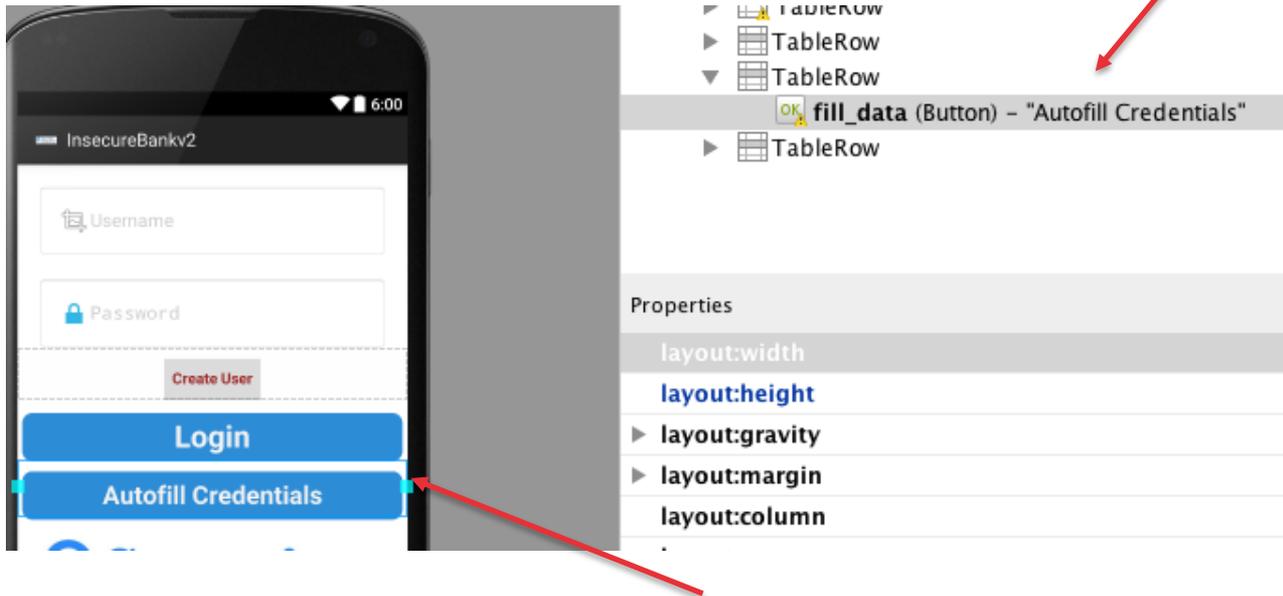
- Método `fillData()`:

```
/*
The function that allows the user to autofill the credentials
if the user has logged in successfully atleast one earlier using
that device
*/
protected void fillData() throws UnsupportedEncodingException, InvalidKeyException {
 // TODO Auto-generated method stub
 // ...
}
```

## Almacenamiento de credenciales

### Solución

- Se elimina el elemento correspondiente del Layout *res/activity\_log\_main.xml*



## Almacenamiento de credenciales

### Solución

- Desde Android 6.0 se puede utilizar el KeyStore del sistema para generar claves simétricas que permitan proteger ciertos secretos del dispositivo:
  - Una vez el dispositivo se ha autenticado recibe un token de autenticación del servidor.
  - Utilizando el KeyStore, se genera una clave con la que se cifra el *token*.
  - El *token* cifrado es almacenado en la memoria interna del dispositivo.
  - Cada vez que la clave sea requerida se le solicitará al usuario el código de bloqueo.
- A continuación se muestra el código para la creación de una clave que requiera al usuario introducir el código de bloqueo cada vez que se vaya a utilizar.

```
KeyGenParameterSpec.Builder builder = new KeyGenParameterSpec.Builder("claveapp",
 KeyProperties.PURPOSE_ENCRYPT | KeyProperties.PURPOSE_DECRYPT);
KeyGenParameterSpec keySpec = builder
 .setKeySize(256)
 .setBlockModes("CBC")
 .setEncryptionPaddings("PKCS7Padding")
 .setRandomizedEncryptionRequired(true)
 .setUserAuthenticationRequired(true)
 .setUserAuthenticationValidityDurationSeconds(5 * 60)
 .build();
KeyGenerator kg = KeyGenerator.getInstance("AES", "AndroidKeyStore");
kg.init(keySpec);
SecretKey key = kg.generateKey();
```

## Almacenamiento de credenciales

### Solución

La aplicación también guarda un fichero por cada movimiento de la cuenta en la tarjeta SD.

- Para incrementar la seguridad de esos datos se modifica el directorio en el que se guardan los ficheros a la *sandbox* de la aplicación.
- En la actividad *DoTransfer*:

```
JSONObject = new JSONObject(result);
acc1 = jsonObject.getString("from");
acc2 = jsonObject.getString("to");
System.out.println("Message:" + jsonObject.getString("message") + " From:" + from.getText().toString() + " To:" + to.getText().toString());
final String status = new String("\nMessage:" + "Success" + " From:" + from.getText().toString() + " To:" + to.getText().toString());
try {
 // Captures the successful transaction status for Transaction history tracking
 String MYFILE = Environment.getExternalStorageDirectory() + "/" + "Statements_" + usernameBase64ByteString + ".html";
 BufferedWriter out2 = new BufferedWriter(new FileWriter(MYFILE, true));
 out2.write(status);
 out2.write("<hr>");
}
```

- En la actividad *ViewStatement*:

```
Intent intent = getIntent();
uname = intent.getStringExtra("uname");
//String statementLocation=Environment.getExternalStorageDirectory()+ "/" + "Statements_" + uname + ".html";
String FILENAME="Statements_" + uname + ".html";
File fileToCheck = new File(Environment.getExternalStorageDirectory(), FILENAME);
System.out.println(fileToCheck.toString());
if (fileToCheck.exists()) {
 //Toast.makeText(this, "Statement Exists!!",Toast.LENGTH_LONG).show();

 WebView mWebView = (WebView) findViewById(R.id.webView1);
 // Location where the statements are stored locally on the device sdcard
 mWebView.loadUrl("file://" + Environment.getExternalStorageDirectory() + "/" + "Statements_" + uname + ".html");
 mWebView.getSettings().setJavaScriptEnabled(true);
 mWebView.getSettings().setSaveFormData(true);
 mWebView.getSettings().setBuiltInZoomControls(true);
}
```

### Eliminación de funcionalidad de administrador

- Durante la tarea anterior se ha visto que existe un botón que no se muestra por defecto en la aplicación y que permite la creación de usuarios dentro de la aplicación.

#### **Tarea**

Elimina toda la funcionalidad oculta de la actividad de *login* en la aplicación móvil que pueda permitir a atacantes, abusar del servicio mediante procesos de ingeniería inversa.

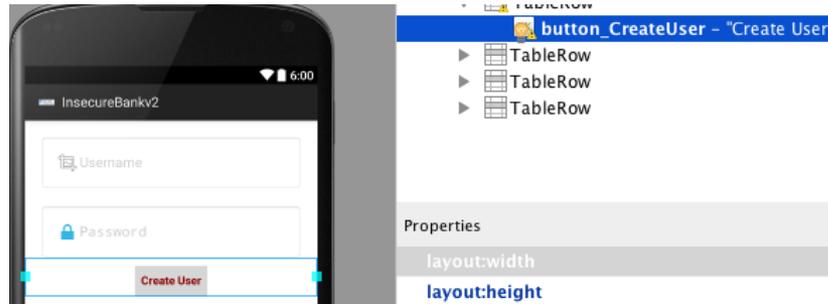
#### **Resultado esperado**

El código de la aplicación móvil sin funcionalidades ocultas en la actividad de *Login*.

## Eliminación de funcionalidad de administrador

### Solución

- En el fichero de *layout* se debe eliminar el botón añadido:



- Aunque comprobando el código no existe ninguna funcionalidad especial añadida, se elimina el código relativo al botón:

```
// The Button that calls the create user function
Button createuser_buttons;

createuser_buttons = (Button) findViewById(R.id.button_CreateUser);
createuser_buttons.setOnClickListener((v) -> {
 // TODO Auto-generated method stub
 createUser();
});
```

### Eliminación de fugas de información a través de los *logs*

- En esta tarea se van a eliminar las posibles fugas de información que se produzcan por la consola del dispositivo durante la ejecución de la aplicación.

#### **Tarea**

Elimina todas las fugas de información sensible que se puedan generar durante la ejecución de la aplicación.

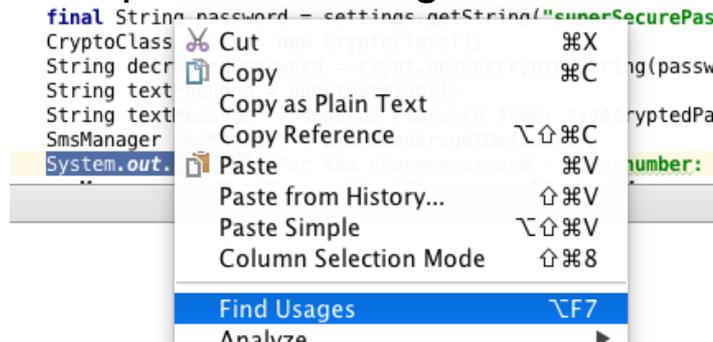
#### **Resultado esperado**

El código de la aplicación sin llamadas a los *logs* o la consola con información que pueda ser considerada como sensible.

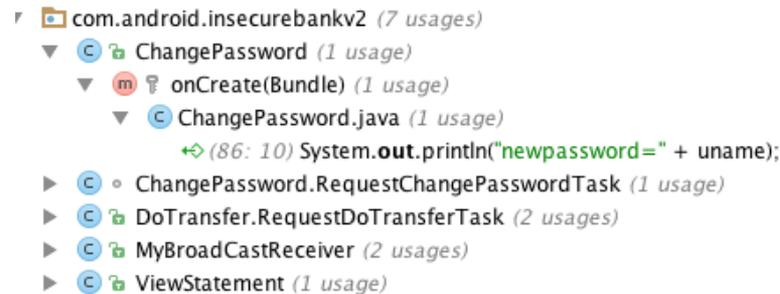
## Eliminación de fugas de información a través de los *logs*

### Solución

- En primer lugar procedemos a buscar todos los usos de System.out en la aplicación mediante la opción findUsages.



- Se obtienen los siguientes resultados, que son eliminados tras su inspección.



## Eliminación de fugas de información a través de los *logs*

### Solución

- De la misma manera se realiza una búsqueda de los usos de la clase Log dentro de la aplicación obteniéndose el resultado siguiente (si no se ha eliminado anteriormente la entrada del Login).

The screenshot displays a search result for the `Log` class. The tree structure is as follows:

- ▼ Class
  - Log
- ▼ Found usages (2 usages)
  - ▼ Nested class access (1 usage)
    - ▼ app (1 usage)
      - ▼ com.android.insecurebankv2 (1 usage)
        - ▼ DoLogin.RequestTask (1 usage)
          - ▼ postData(String) (1 usage)
            - ▼ DoLogin.java (1 usage)
              - ↔ (149: 6) `Log.d("Successful Login:", ", account=" + username + ":" + password);`

- ▶ Usage in import (1 usage)

## Permisos

- Siguiendo el principio de menor número de privilegios, en esta tarea se van a eliminar aquellos permisos que la aplicación no requiera para su ejecución.

### **Tarea**

Analiza el uso de cada uno de los permisos en la aplicación y elimínalos si no son necesarios para el correcto funcionamiento de la misma.

### **Resultado esperado**

Un manifest actualizado con la lista de permisos estrictamente necesaria para la ejecución de la aplicación.

## Permisos

### Solución

- La aplicación utiliza los siguientes permisos:

```
<uses-permission android:name="android.permission.INTERNET" />
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.SEND_SMS" />

<!--
 To retrieve OAuth 2.0 tokens or invalidate tokens to disconnect a user. This disconnect
 option is required to comply with the Google+ Sign-In developer policies
-->
<uses-permission android:name="android.permission.USE_CREDENTIALS" /> <!-- To retrieve the acc
<uses-permission android:name="android.permission.GET_ACCOUNTS" /> <!-- To auto-complete the e
<uses-permission android:name="android.permission.READ_PROFILE" />
<uses-permission android:name="android.permission.READ_CONTACTS" />

<android:uses-permission android:name="android.permission.READ_PHONE_STATE" />
<android:uses-permission
 android:name="android.permission.READ_EXTERNAL_STORAGE"
 android:maxSdkVersion="18" />
<android:uses-permission android:name="android.permission.READ_CALL_LOG" />

<application
 android:allowBackup="true"
 android:icon="@mipmap/ic_launcher"
 android:label="@string/app_name"
 android:theme="@android:style/Theme.Holo.Light.DarkActionBar">
```

## Permisos

### Solución

- El permiso de Internet es necesario para que la aplicación se pueda conectar al *back-end* del banco por lo que se mantiene.
- El almacenamiento externo era utilizado para almacenar los movimientos. Al haber modificado su lugar de almacenamiento se pueden eliminar los permisos de lectura y escritura de la tarjeta SD.
- El permiso de envío de SMS ya no es necesario, pues esas operaciones se deberían realizar desde una pasarela en el *back-end*.
- La aplicación en ningún momento necesita acceder a los credenciales del dispositivo. En su configuración actual los credenciales no son almacenados, y en el caso de que lo fuesen, se trataría credenciales propios de la aplicación y no se necesitaría solicitar ningún permiso adicional para su acceso. Se procede a eliminar los permisos GET\_ACCOUNTS y USE\_CREDENTIALS.

## Permisos

### Solución

- Los permisos relativos al teléfono y el historial de llamadas se necesitan para que la aplicación sepa el número de teléfono al que mandarle el SMS una vez se ha modificado la contraseña. En la actividad *ChangePassword* se puede observar el siguiente código:

```
TelephonyManager phoneManager = (TelephonyManager)getApplicationContext().getSystemService(Context.TELEPHONY_SERVICE);
String phoneNumber = phoneManager.getLine1Number();
System.out.println("pho: "+phoneNumber);
```

- Debido a que ya no es necesario se elimina junto con los permisos asociados:

```
<uses-permission android:name="android.permission.READ_PROFILE" />
<uses-permission android:name="android.permission.READ_CONTACTS" />

android:uses-permission android:name="android.permission.READ_PHONE_STATE" />
```

- Se puede comprobar también que hay permisos mal definidos en la aplicación (empiezan en android). Se procede también a su eliminación.
- El permiso de lectura de contactos no es necesario, pues la aplicación no necesita acceder a los mismos.
- El único permiso que queda en el manifest es el permiso de INTERNET.

## Tarea adicional

- Además de las tareas anteriores, se pueden efectuar otras tareas que mejorarían la seguridad de la aplicación estudiada.
- Como tarea adicional, se propone la implementación de *certificate pinning* en la aplicación cliente.
- Para ello se recomienda seguir los siguientes pasos:
  - Se tiene que modificar el código de la aplicación servidor para ofrecer conexiones por SSL (<http://flask.pocoo.org/snippets/111/>).
  - Será necesaria la creación de un par de claves pública y privada con su correspondiente certificado.
  - Finalmente, se añadiría el pinning a la aplicación como se ha explicado anteriormente en la unidad.
    - Hay que tener en cuenta que al realizar el *pinning*, no es necesario que el certificado esté firmado por una CA ya registrada en el dispositivo.
- Si se decide completar, se recomienda compartir la solución alcanzada en el foro correspondiente.



# Laboratorio de iOS

## Procedimiento

<input checked="" type="checkbox"/>	_____

- Las tareas a efectuar durante este laboratorio son las siguientes:
  - Preparación del entorno de trabajo.
  - Almacenamiento de credenciales.
  - Evitar la manipulación en tiempo de ejecución.
  - Eliminación de funcionalidad de administrador.
  - Eliminación de fugas de información a través de los *logs*.
  - Permisos.

## Preparación del entorno

- Esta tarea se debe realizar en un equipo con Mac OS X configurado como se describió en la unidad 0 del curso.
- Para no interferir con los resultados del análisis que se realizó en la unidad 3, se crea una carpeta dentro del directorio de documentos con el nombre “laboratorio\_ios”.
  - > cd Documents
  - > mkdir laboratorio\_ios
  - > Cd laboratorio\_ios
- Se clona el repositorio:
  - > git clone https://github.com/prateek147/DVIA.git
  - > cd DVIA
- Se abre *DVIA/DamnVulnerableIOSApp/DamnVulnerableIOSApp.xcodeproj* con Xcode.

## Almacenamiento de datos

- En esta tarea se va a revisar el código del método `saveInUserDefaultsTapped` para evitar que la información sea guardada en claro en un fichero mediante el uso de `NSUserDefaults`.

### Tarea

En el fichero `InsecureDataStorageVulnVC` modifica el método `saveInUserDefaultsTapped` para que guarde la información se guarde de forma segura en el dispositivo.

### Resultado esperado

La información introducida en el campo debe ser guardada de forma segura en el dispositivo.

## Almacenamiento de datos

### Solución

- En primer lugar estudiamos el código del método mencionado en el enunciado:

```
- (IBAction)saveInUserDefaultsTapped:(id)sender {
 NSMutableDictionary *defaults = [NSMutableDictionary standardUserDefaults];
 [defaults setObject:self.userDefaultsTextField.text forKey:@"DemoValue"];
 [defaults synchronize];
 [DamnVulnerableAppUtilities showAlertWithMessage:@"Data saved in UserDefaults"];
}
```

- El mejor método de almacenamiento para evitar que la información se almacene en claro es almacenar los datos en el KeyChain del dispositivo.
- Para ello se puede utilizar directamente la API de [KeyChain](#) de Apple.
- Existe una librería ampliamente testada que hace de wrapper para la API del KeyChain llamada [PDKeychainBindingsController](#).
- La librería permite guardar y almacenar los objetos con la misma metodología que los UserDefaults.

```
- (IBAction)saveInUserDefaultsTapped:(id)sender {
 PDKeychainBindings *bindings = [PDKeychainBindings sharedKeychainBindings];
 [bindings setObject:self.keychainTextField.text forKey:@"DemoValue"];
 [DamnVulnerableAppUtilities showAlertWithMessage:@"Data saved in KeyChain"];
}
```

## Evitando la manipulación en tiempo de ejecución

- En esta tarea se va a evitar que atacantes puedan añadir un depurador a la aplicación para modificar su flujo de ejecución.

### **Tarea**

Añade el código necesario a la aplicación para que no puedan utilizarse depuradores durante la ejecución de la aplicación.

### **Resultado esperado**

La aplicación no se podrá cargar cuando se esté utilizando el simulador o un dispositivo que esté conectado para su depuración.

## Evitando la manipulación en tiempo de ejecución

### Solución

- Durante la unidad se ha comprobado que se puede evitar la utilización de un depurador mediante `PT_DENY_ATTACH`.
- Si se quiere evitar que el depurador pueda siquiera inspeccionar el principio de la aplicación, se deberá añadir la llamada a `ptrace` con el parámetro anterior nada más iniciar la aplicación, en el método *main*:

```
int main(int argc, char * argv[])
{
 ptrace(PT_DENY_ATTACH, 0, 0, 0);
 @autoreleasepool {
 return UIApplicationMain(argc, argv, nil, NSStringFromClass([AppDelegate class]));
 }
}
```

- Si se quiere restringir la utilización a ciertos escenarios siempre se pueden añadir directivas al compilador.

```
int main(int argc, char * argv[])
{
#ifdef DEBUG
 ptrace(PT_DENY_ATTACH, 0, 0, 0);
#endif
 @autoreleasepool {
 return UIApplicationMain(argc, argv, nil, NSStringFromClass([AppDelegate class]));
 }
}
```

## Evitando la utilización del portapapeles

- En esta tarea se va a evitar que un usuario pueda copiar información de un campo de texto al portapapeles. En concreto esta tarea se centra en la vista sobre fugas en el portapapeles `SideChannelDataLeakageDetailsVC`.

### Tarea

Modifica la configuración de los campos de la vista

`SideChannelDataLeakageDetailsVC` para que la información de los campos no pueda ser copiada.

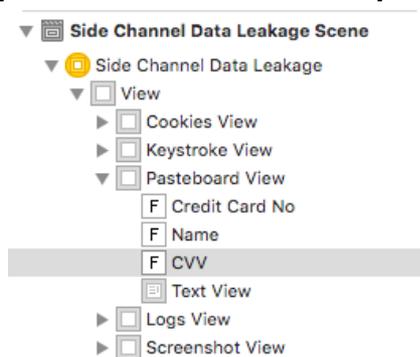
### Resultado esperado

La aplicación no mostrará la opción de copiar en ninguno de los campos que permite la entrada de datos.

## Evitando la manipulación en tiempo de ejecución

### Solución

- Las propiedades de los campos de texto se definen en el fichero de storyboard de la aplicación. Concretamente se definen en el fichero *Main.storyboard*.
- Para modificar las propiedades del campo se debe acceder a la vista correspondiente.



- El campo CVV tiene  Auto-enable Return Key no poder copiar los datos introducidos.  Secure Text Entry

- Modificando las propiedades de los otros campos de la misma manera se consigue evitar que se puedan copiar los datos introducidos al campo.

## *Certificate Pinning*

- Actualmente, la conexión mediante *certificate pinning* falla debido a que el certificado guardado en la aplicación no coincide con el obtenido al realizar la petición a google.co.uk.

### **Tarea**

Modifica la aplicación para que las conexiones que se realizan mediante certificate pinning puedan realizarse correctamente.

### **Resultado esperado**

La aplicación no mostrará la opción de copiar en ninguno de los campos que permite la entrada de datos.

## Certificate Pinning

### Solución

- La primera tarea a realizar es descargar el certificado correcto para poder validarlo desde la aplicación. En esta resolución se va a modificar la aproximación y se va a hacer el pinning mediante el resumen SHA-256 del certificado.
- El resumen se puede calcular desde la propia app modificando el código del delegado `willSendRequestForAuthenticationChallenge` en el controlador `TransportLayerProtectionVC`.

- Aña 

```
NSData *remoteCertificateData = CFBridgingRelease(SecCertificateCopyData(certificate));
NSMutableData *macOut = [NSMutableData dataWithLength:CC_SHA256_DIGEST_LENGTH];

CC_SHA256(remoteCertificateData.bytes, remoteCertificateData.length, macOut.mutableBytes);

NSLog(@"macOut: %@", macOut);
```

- Se obtiene por el log el resumen del certificado  

```
2016-02-22 23:59:45.926 DamnVulnerableIOSApp[3100:666535]
macOut: <71923f11 3890a377 4ac55b67 33a41d10 bc4014bc 74c7229a
e4e78507 ef0efa98>
```

## Certificate Pinning

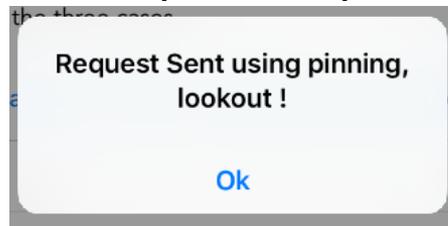
### Solución

- Ahora basta con modificar el código para cambiar la comprobación que se realiza durante la conexión para que se compruebe el certificado recibido.

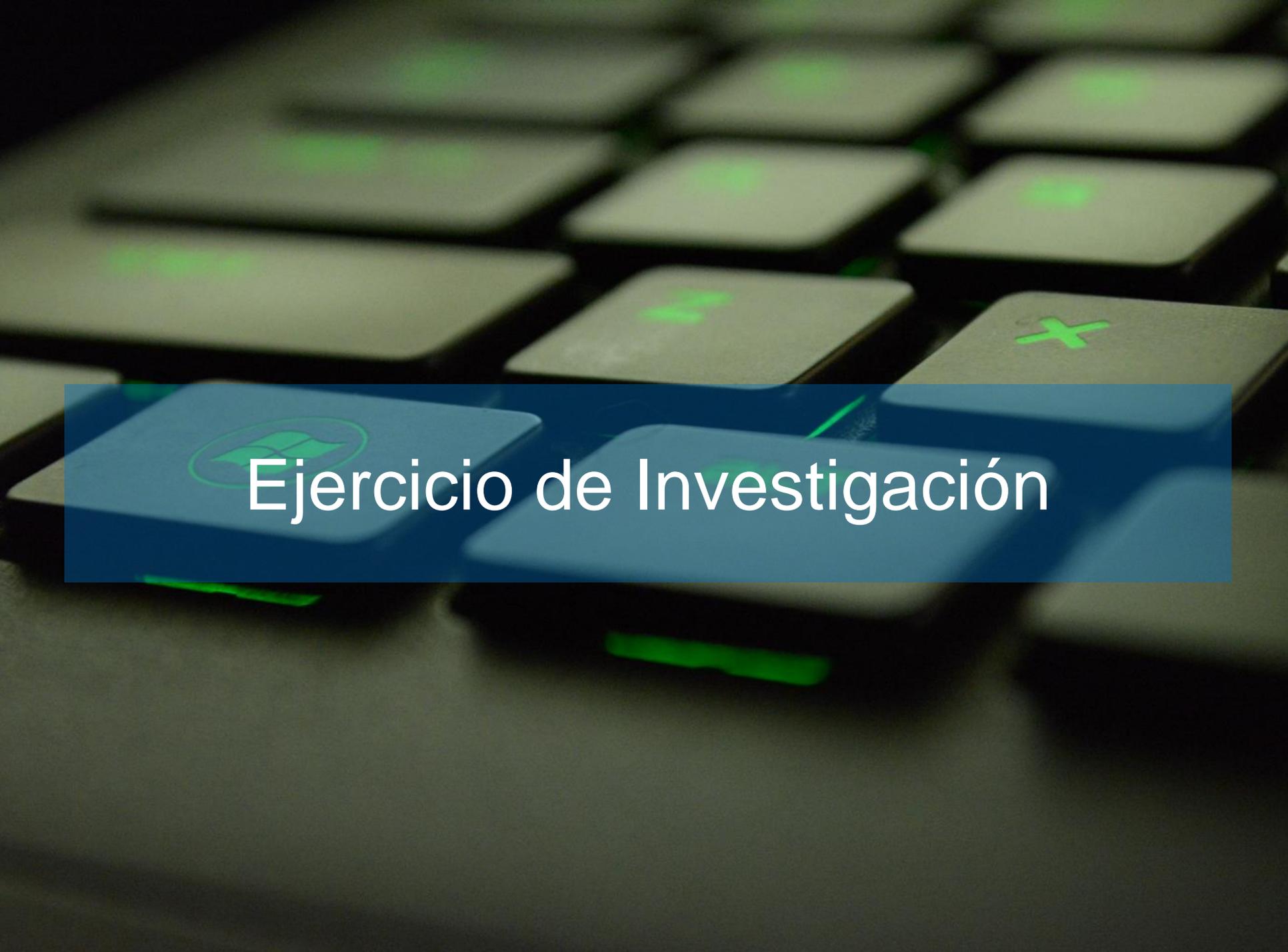
```
NSData *remoteCertificateData = CFBridgingRelease(SecCertificateCopyData(certificate));
NSMutableData *macOut = [NSMutableData dataWithLength:CC_SHA256_DIGEST_LENGTH];
CC_SHA256(remoteCertificateData.bytes, remoteCertificateData.length, macOut.mutableBytes);
NSString *pin= @"71923f113890a3774ac55b6733a41d10bc4014bc74c7229ae4e78507ef0efa98";
NSUInteger dataLength = [macOut length];
NSMutableString *remoteHashString = [NSMutableString stringWithCapacity:dataLength*2];
const unsigned char *dataBytes = [macOut bytes];
for (NSUInteger idx = 0; idx < dataLength; ++idx) {
 [remoteHashString appendFormat:@"%02x", dataBytes[idx]];
}

if ([remoteHashString isEqualToString:pin]) {
 [DamnVulnerableAppUtilities showAlertWithMessage:@"Request Sent using pinning, lookout !"];
 NSURLCredential *credential = [NSURLCredential credentialForTrust:serverTrust];
 [[challenge sender] useCredential:credential forAuthenticationChallenge:challenge];
}
```

- Ejecutando la aplicación se comprueba que la validación funciona correctamente.



- Esta tarea también se puede resolver mediante la utilización de [TrustKit](#).



# Ejercicio de Investigación

# ◆◆◇ Ejercicio de Investigación

## Enunciado

- Durante este ejercicio se deberá realizar una labor de investigación y volcar en el foro de la asignatura los resultados obtenidos para el debate con el resto de alumnos.
  - Como se ha podido comprobar durante la unidad y los diferentes laboratorios, el almacenamiento de los datos en el dispositivo es uno de los grandes retos para la seguridad de los mismos hasta el punto de que muchas de las aplicaciones incorporan funciones de cifrado para la protección de todos sus datos, no únicamente de las credenciales.
  - En este ejercicio de investigación se pide:
    - Identificar, a semejanza de lo estudiado para Android e iOS, los mecanismos de protección de datos en reposo con los que cuentan los sistemas operativos Windows Phone y BlackBerry 10.
    - Identificar, justificando la respuesta, cuál es el eslabón más débil en la protección de estos datos y bajo que circunstancias un atacante puede recuperarlos. Esta tarea se deberá realizar para los cuatro sistemas operativos Windows Phone, BlackBerry 10, Android e iOS.

A hand holding a pen is positioned over an open notebook. In the foreground, a black calculator is placed on the notebook's pages. The notebook contains mathematical problems, including arithmetic series and word problems. A semi-transparent blue banner is overlaid across the middle of the image, containing the text 'Test de evaluación'.

# Test de evaluación

26.  $1 + 5 + 9 + \dots + 401$   
28.  $(-30) + (-35) + (-20) + \dots + 79$   
30.  $2 + 13 + 24 + \dots + 79$   
32. the first 30 terms of the series

34.  $\sum_{n=1}^{10} (2n - 4)$   
39.  $2 + 9 + 16 + \dots + 65$   
41.  $80 + 76 + 72 + \dots +$

partial sum  $S_{15}$  of the arithmetic series  $7 + 11 + 15 + 19 + \dots$   
the partial sum  $S_{100}$  of the arithmetic series  $1 + 1.25 + 1.5 + 1.75 + \dots$   
each arithmetic series in sigma notation and find its sum.  
the seventeenth hexagonal number, which is equal to  $S_{17}$  for the  
Nation in a country experiencing runaway inflation, the cost  
of a tomato on January 1 of a non-leap year a tomato  
during the year?  
the first five terms of the sequence graphed at  
\$0 for the first parking offense. The fine  
subsequent offense.  
driver would pay for ten offenses.

# Gracias por su atención

