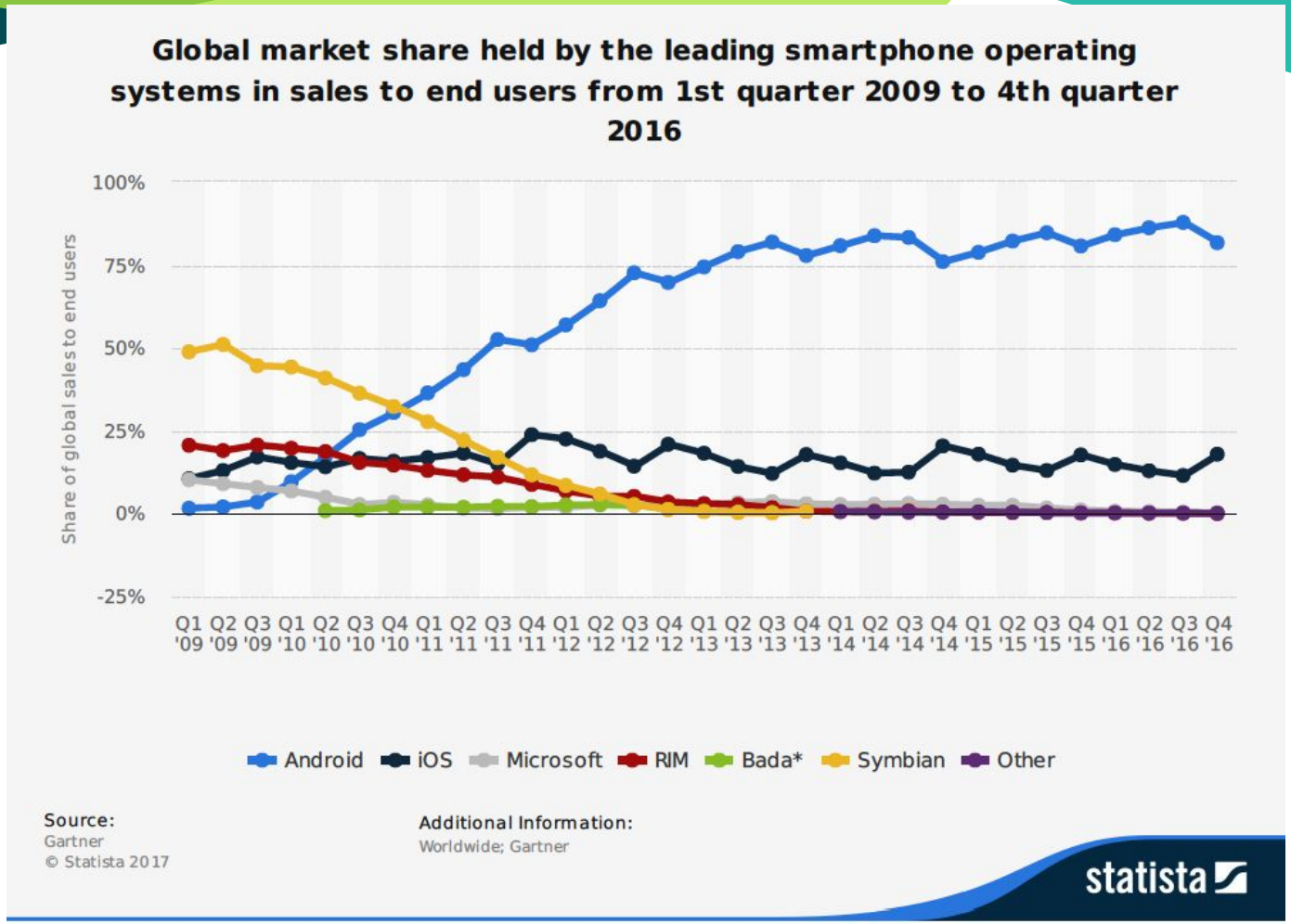
Seguridad en Sistemas Móviles

ESIIAB - UCLM

Pedro Gómez López

Seguridad de Sistemas Software

Contexto

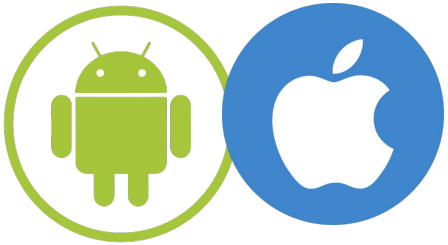

Global market share held by the leading smartphone operating systems in sales to end users from 1st quarter 2009 to 4th quarter 2016
Share of global sales to end users
100%
75%
50%
25%
0%
-25%
Q1 '09 Q2 '09 Q3 '09 Q1 '10 Q2 '10 Q3 '10 Q4 '10 Q1 '11 Q2 '11 Q3 '11 Q4 '11 Q1 '12 Q2 '12 Q3 '12 Q4 '12 Q1 '13 Q2 '13 Q3 '13 Q4 '13 Q1 '14 Q2 '14 Q3 '14 Q4 '14 Q1 '15 Q2 '15 Q3 '15 Q4 '15 Q1 '16 Q2 '16 Q3 '16 Q4 '16
Android
iOS
Microsoft
RIM
Bada*
Symbian
Other
Source:
Gartner
© Statista 2017
Additional Information:
Worldwide; Gartner
statista

Objetivos

Conocer los mecanismos principales de seguridad en Android

Seguridad en Android, atendiendo a lenguajes de programación

Experimentando con permisos en Android



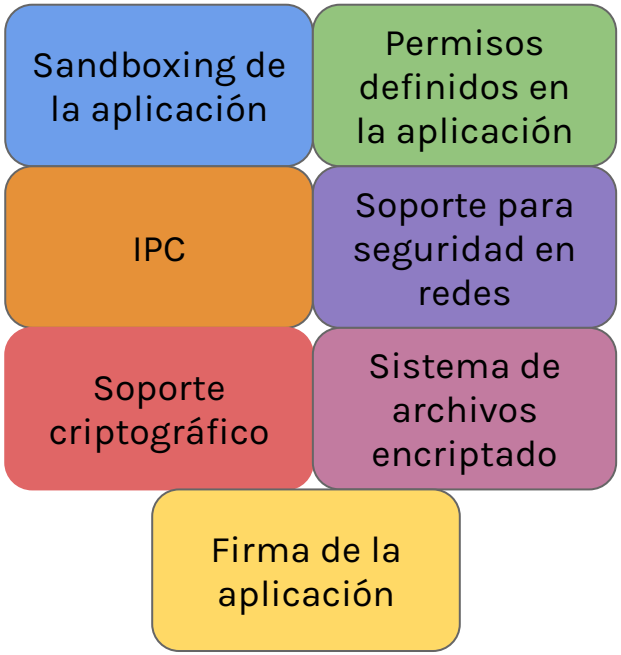
Android VS iOS en términos de seguridad

Vulnerabilidad Stagefright

Un poco de curiosidad...

Algunos conceptos teóricos

Principales mecanismos de seguridad en Android

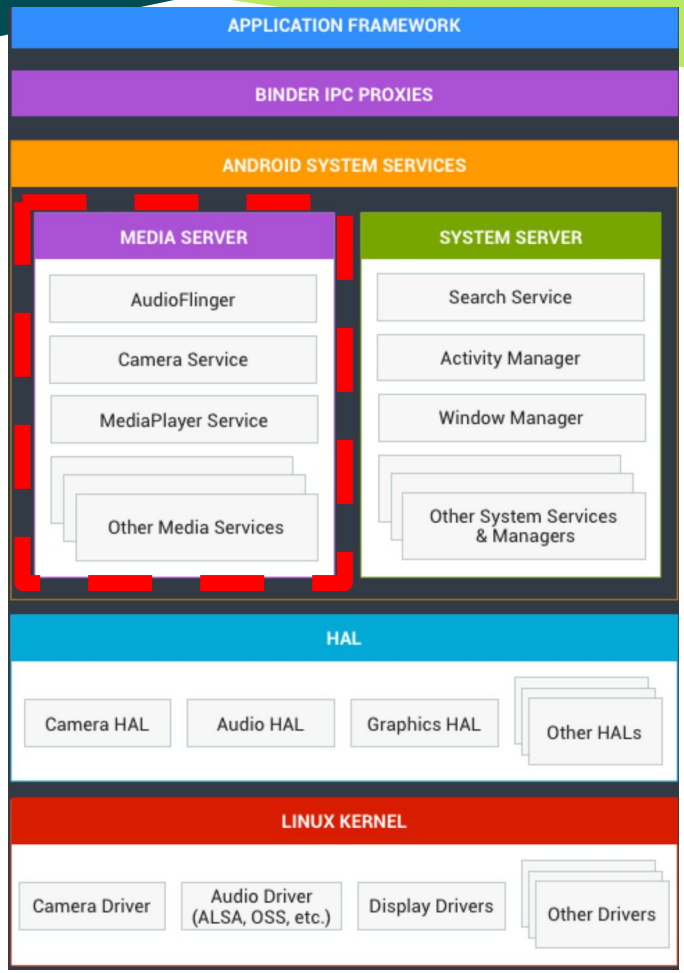


Algunos conceptos teóricos

Seguridad en Android, una aproximación teniendo en cuenta el lenguaje

- **Gestión de memoria**
- **Inicialización de variables**
- **Métodos de acceso**
- **Tipos de casts**
- **Vectores**
- **JNI y código nativo**

Vulnerabilidad Stagefright



- Librería multimedia escrita en (C++)
- Un proceso se ejecuta con gran cantidad de privilegios (potencialmente de tipo “system”)
- Extracción de metadatos
- 11+ ataques a vectores (incl. MMS)
- Procesamiento de contenido multimedia antes de ser notificado
- Vulnerable a través de corrupción de memoria
- Ejemplo: memoria asignada insuficiente por *integer overflow*

Algunos conceptos teóricos

Android VS iOS en términos de seguridad

Experimentando con permisos en Android

Palabras clave

Android
JavaScript
WebView
HTML
Permisos

Permisos en tiempo de ejecución

Tenemos que tratarlos con gran atención y cuidado

<Código más importante>

```
<!-- PERMISSIONS DEFINITION -->
<uses-permission android:name="android.permission.INTERNET" />
<uses-permission android:name="android.permission.READ_PHONE_STATE" />
```

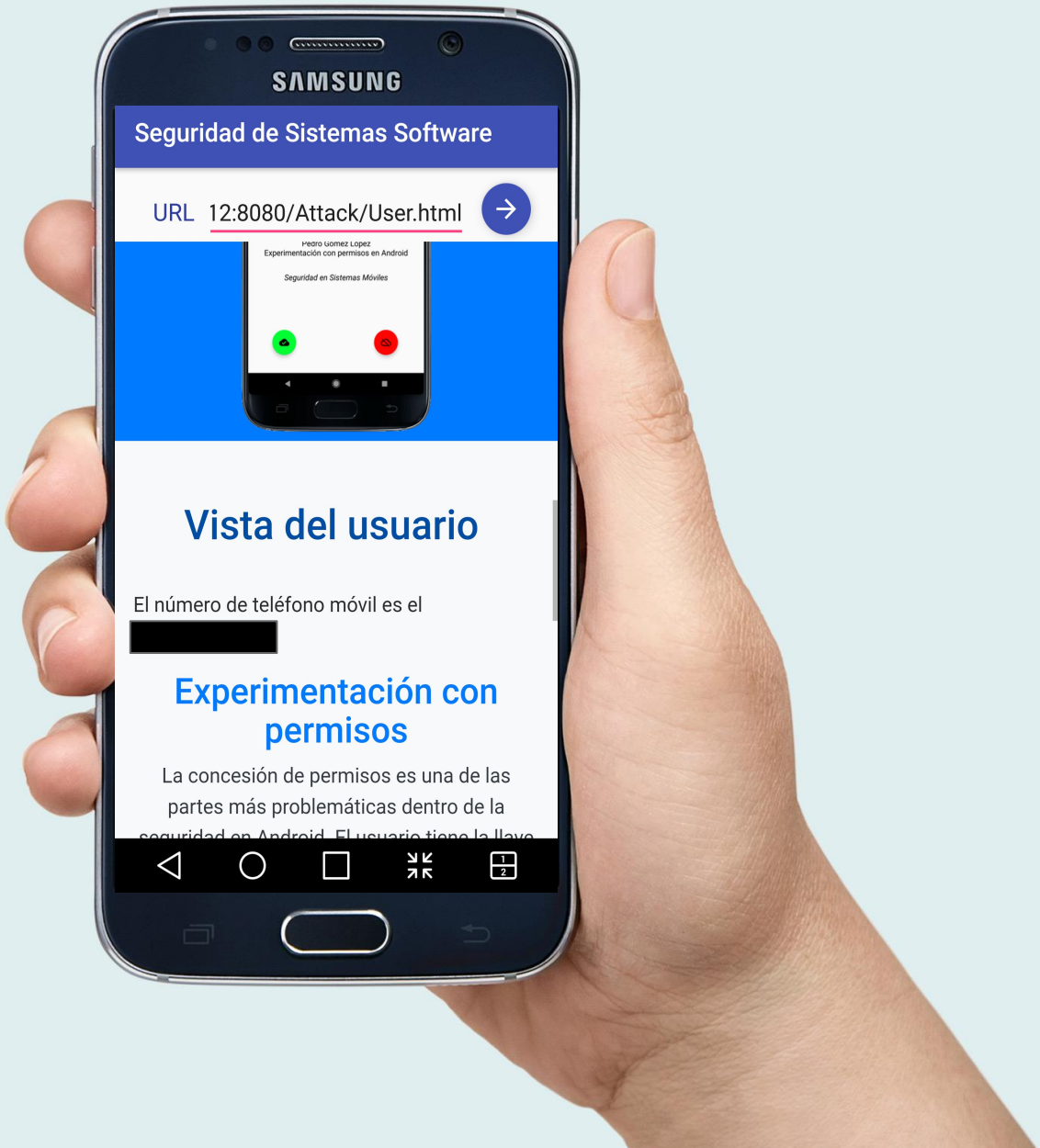
```
//Enable Javascript
webpage.getSettings().setJavaScriptEnabled(true);
//Inject WebAppInterface methods into Web page by having Interface name 'Android'
webpage.addJavascriptInterface(new SafeFragment.WebAppInterface(), "Android");
```

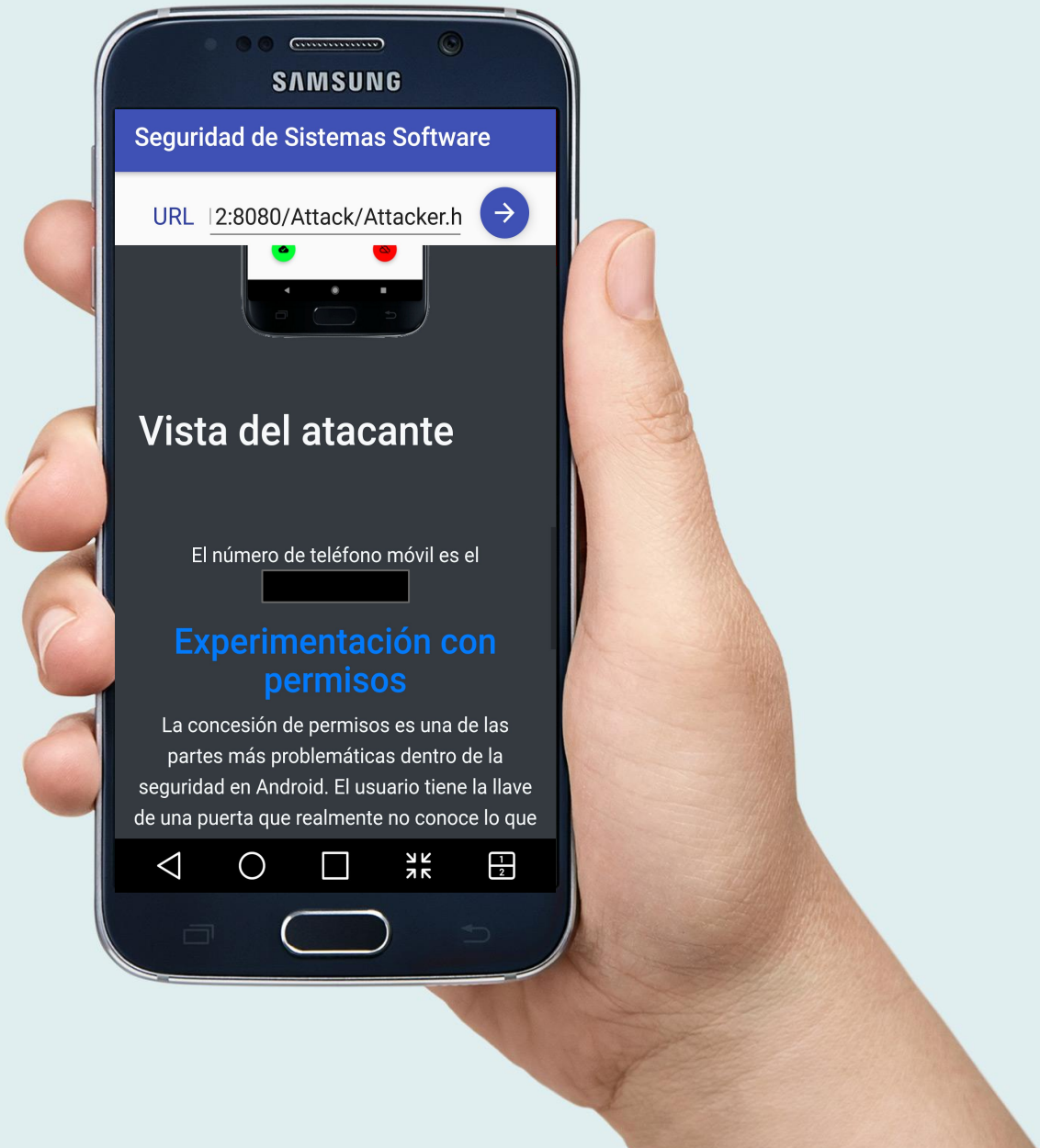
<Código más importante>

```
// Class to be injected in Web page
public class WebAppInterface {
    //This method return user phone number to the javascript calls from website
    @JavascriptInterface
    public String GetPhoneNumber() {
        return GetUserPhoneNumber();
    }
}

/* Method for getting the user phone number from the device */
String GetUserPhoneNumber() {
    TelephonyManager tMgr = (TelephonyManager) getSystemService(Context.TELEPHONY_SERVICE);
    String mPhoneNumber = tMgr.getLine1Number();
    return mPhoneNumber;
}
```

```
<!-- Parte necesaria para el experimento -->
<script type="text/javascript">
  function GetPhoneNumber() {
  // Gettting user phone number from android device
  var PhoneNumber= Android.GetPhoneNumber();
  document.getElementById("phone").innerHTML="El número de teléfono móvil es el "+ PhoneNumber;
  }
  // Call get phone number function
  GetPhoneNumber();
</script>
<!-- Parte necesaria para el experimento -->
```


SAMSUNG
Seguridad de Sistemas Software
URL 12:8080/Attack/User.html
Pedro Gomez Lopez
Experimentación con permisos en Android
Seguridad en Sistemas Móviles
Vista del usuario
El número de teléfono móvil es el
Experimentación con permisos
La concesión de permisos es una de las partes más problemáticas dentro de la


SAMSUNG
Seguridad de Sistemas Software
URL 2:8080/Attack/Attacker.h
Vista del atacante
El número de teléfono móvil es el
[redacted]
Experimentación con permisos
La concesión de permisos es una de las partes más problemáticas dentro de la seguridad en Android. El usuario tiene la llave de una puerta que realmente no conoce lo que


// Class to be injected in Web page
public class WebAppInterface {
//This method return user phone number to the javascript calls from website
@JavascriptInterface
public String GetPhoneNumber() {
// Only send the phone to authorize website
if(URL.getText().toString().indexOf(HostingURL)==0)
return GetUserPhoneNumber();//
else
return null;
}
}
Vista del atacante
El número de teléfono móvil es el
[redacted]
Experimentación con permisos
La concesión de permisos es una de las partes más problemáticas dentro de la seguridad en Android. El usuario tiene la llave de una puerta que realmente no conoce lo que
Vista del atacante
El número de teléfono móvil es el undefined
Experimentación con permisos
La concesión de permisos es una de las partes más problemáticas dentro de la seguridad en Android. El usuario tiene la llave de una puerta que realmente no conoce lo que esconde.

DEMO EN DIRECTO

Herramientas para replicar el experimento

VirtualBox para importar la máquina virtual con la configuración ya cargada

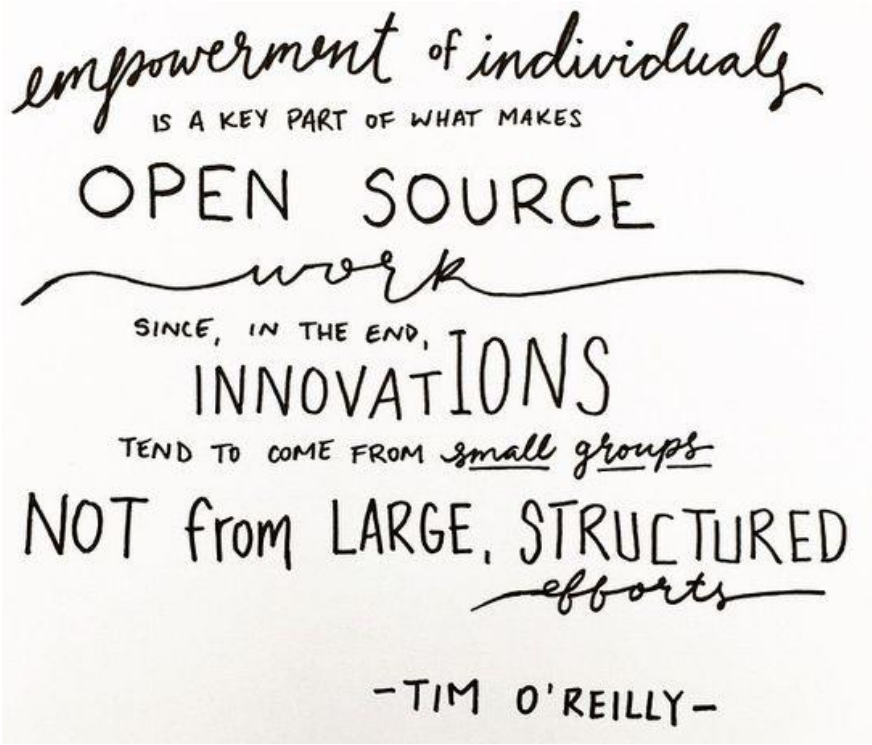
Android Studio para jugar con la aplicación (sobre todo temas de IPs) y poder realizar más pruebas

Un terminal con Android para probar en un entorno real la funcionalidad de la aplicación

Un ordenador para levantar el servidor Apache de la máquina virtual con las correspondientes páginas web

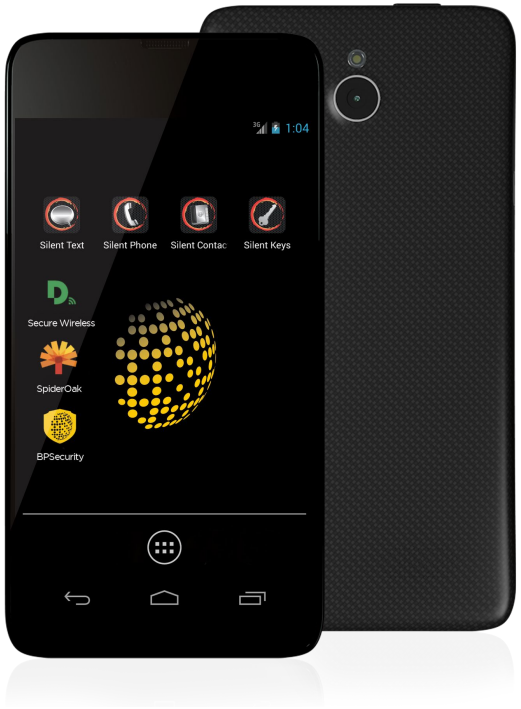
Open source

pegomez



Un poco de curiosidad

Blackphone



silent circle

Un poco de curiosidad

Kotlin

Kotlin

UBER

Consideraciones finales

- A nivel de sistema, existen numerosos problemas de seguridad
- La mayoría de los problemas de seguridad en sistemas móviles se deben a la educación (**o más bien la falta de educación**) de los usuarios finales
- iOS es más seguro en el sentido que **deja en manos del usuario menos decisiones**
- Enviar datos sensibles solamente a páginas web y sitios en que confiemos, o que cuenten con la certificación de calidad y seguridad

Bibliografía

[1] Gartner, "**Global mobile os market share in sales to end users from 1st quarter 2009 to 1st quarter 2016**," 2017. Disponible desde: https://www.statista.com/statistics/266136/global-market-share-held-by-smartphone-operating-systems/ Última vez accedido el: 05-12-2017.

[2] V. Savov, "**Android's popularity eclipses windows among internet users,**" 2017. Disponible desde: https://www.theverge.com/2017/4/3/15159320/android-windows-internet-usage-statistics-competition. Última vez accedido el: 05-12-2017.

[3] N. Elenkov, ***Android Security Internals, An In-Depth Guide to Android's Security Architecture***. San Francisco: No Starch Press, 2015.

[4] K. Yaghmour, ***Embedded Android***. Sebastopol: O'Reilly, 2013.

[5] "**Art and dalvik**." Disponible desde: https://source.android.com/devices/tech/dalvik/. Última vez accedido el: 06-12-2017.

[6] B. Cruz Zapata and A. Hernandez Niñirola, ***Testing and Securing Android Studio Applications***. Birmingham: Packt Publishing Ltd., 2014.

[7] "**Security tips**." Disponible desde: https://developer.android.com/training/articles/security-tips.html. Último vez accedido el: 06-12-2017.

[8] "**Encryption**." Disponible desde: https://source.android.com/security/encryption/. Último vez accedido el: 06-12-2017.

[9] "**Application signing**." Disponible desde: https://source.android.com/security/apksigning/. Última vez accedido el: 06-12-2017.

[10] "**App manifest.**" Disponible desde: https://developer.android.com/guide/topics/manifest/manifest-element.html#uid. Última vez accedido el: 06-12-2017.

Bibliografía

[11] "**Jni tips.**" Disponible desde: https://developer.android.com/training/articles/perf-jni.html Última vez accedido el: 06-12-2017.

[12] "**Android ndk.**" Available from: https://developer.android.com/ndk/index.html. Última vez accedido el: 06-12-2017.

[13] "**Design goals of the java programming language.**" Disponible desde: http://www.oracle.com/technetwork/java/intro-141325.html. Última vez accedido el: 07-12-2017.

[14] "**Main features of the java programming language.**" Disponible desde: http://www.oracle.com/technetwork/java/simple-136065.html. Último vez accedido el: 07-12-2017.

[15] "**Java - primitive data types.**" Disponible desde: https://docs.oracle.com/javase/tutorial/java/nutsandbolts/datatypes.html. Última vez accedido el: 08-12-2017.

[16] "**Java - controlling access to members of a class.**" Disponible desde: https://docs.oracle.com/javase/tutorial/java/javaOO/accesscontrol.html . Última vez accedido el: 08-12-2017.

[17] "**Java - conversions and promotions.**" Disponible desde: https://docs.oracle.com/javase/specs/jls/se7/html/jls-5.html . Última vez accedido el: 08-12-2017.

[18] "**Owasp homepage.**" Disponible desde: https://www.owasp.org/index.php/Main_Page . Última vez accedido el: 08-12-2017.

[19] "**Owasp - unsafe jni.**" Disponible desde: https://www.owasp.org/index.php/Unsafe_JNI . Última vez accedido el: 08-12-2017.

[20] "**Black hat homepage.**" Disponible desde: https://www.blackhat.com/. Última vez accedido el: 08-12-2017.

Bibliografía

[21] "**Presentation slides of Joshua Drake's black hat talk.**" Disponible desde: https://www.blackhat.com/docs/us-15/materials/36us-15-Drake-Stagefright-Scary-Code-In-The-Heart-Of-Android.pdf . Última vez accedido el: 09-12-2017.

[22] "**Video recording of joshua drake's black hat talk.**" Disponible desde: https://www.facebook.com/profile.php?id=100013285597091 . Última vez accedido el: 09-12-2017.

[23] "**Security enhancements in android 1.5 through 4.1.**" Disponible desde: https://source.android.com/security/enhancements/enhancements41 . Última vez accedido el: 09-12-2017.

[24] "**Google play store link to zimperiums stagefright detector.**" Disponible desde: https://play.google.com/store/apps/details?id=com.zimperium.stagefrightdetector&hl=de . Última vez accedido el: 09-12-2017.

[25] "**Android - platform versions.**" Disponible desde: https://developer.android.com/about/dashboards/index.html#Platform . Última vez accedido el: 10-12-2017.

[26] I. Mohamed and D. Patel, "**Android vs ios security: A comparative study,**" *12th International Conference on Information Technology - New Generations*, 2015.

[27] R. N. R. H. Mohd Shahdi Ahmad, Nur Emyra Musa and N. E. Othman, "**Comparison Between Android and iOS Operating System in terms of Security,**" *8th International Conference on Information Technology in Asia (CITA)*, 2013.

[28] D. E. Krutz and S. A. Malachowsky, "**Teaching android security through examples: A publicly available database of vulnerable apps,**" *ACM Inroads*, 2016.

[29] "**Blackphone 2.**" Disponible desde: http://sc2016.wpengine.com/products-and-solutions/devices/ . Última vez accedido el: 10-12-2017.

[30] "**Kotlin.**" Disponible desde: https://kotlinlang.org/ . Última vez accedido el: 10-12-2017.

Muchas gracias por vuestra atención.
¿ Alguna pregunta ?