



Nuevas amenazas a las tecnologías móviles

Android APK

Jong Park

2 de Diciembre de 2015



Revisión a las aplicaciones móviles

- Introducción
- Aplicaciones móviles
 - ✓ Importancia
 - ✓ Amenazas
 - ✓ Propuesta
- Caso Real
- Conclusiones



Introducción

- Con base en la importancia que han adquirido las tecnologías móviles en las diferentes organizaciones y la interacción cada vez mayor de los usuarios finales con las organizaciones a través de las aplicaciones e interfaces móviles, el equipo de Cyber Security de Deloitte México realiza revisiones de seguridad extensivas que permiten la identificación oportuna del nivel de riesgo al que la información puede estar expuesta.



Aplicaciones Móviles

Importancias y amenazas

Aplicaciones Móviles

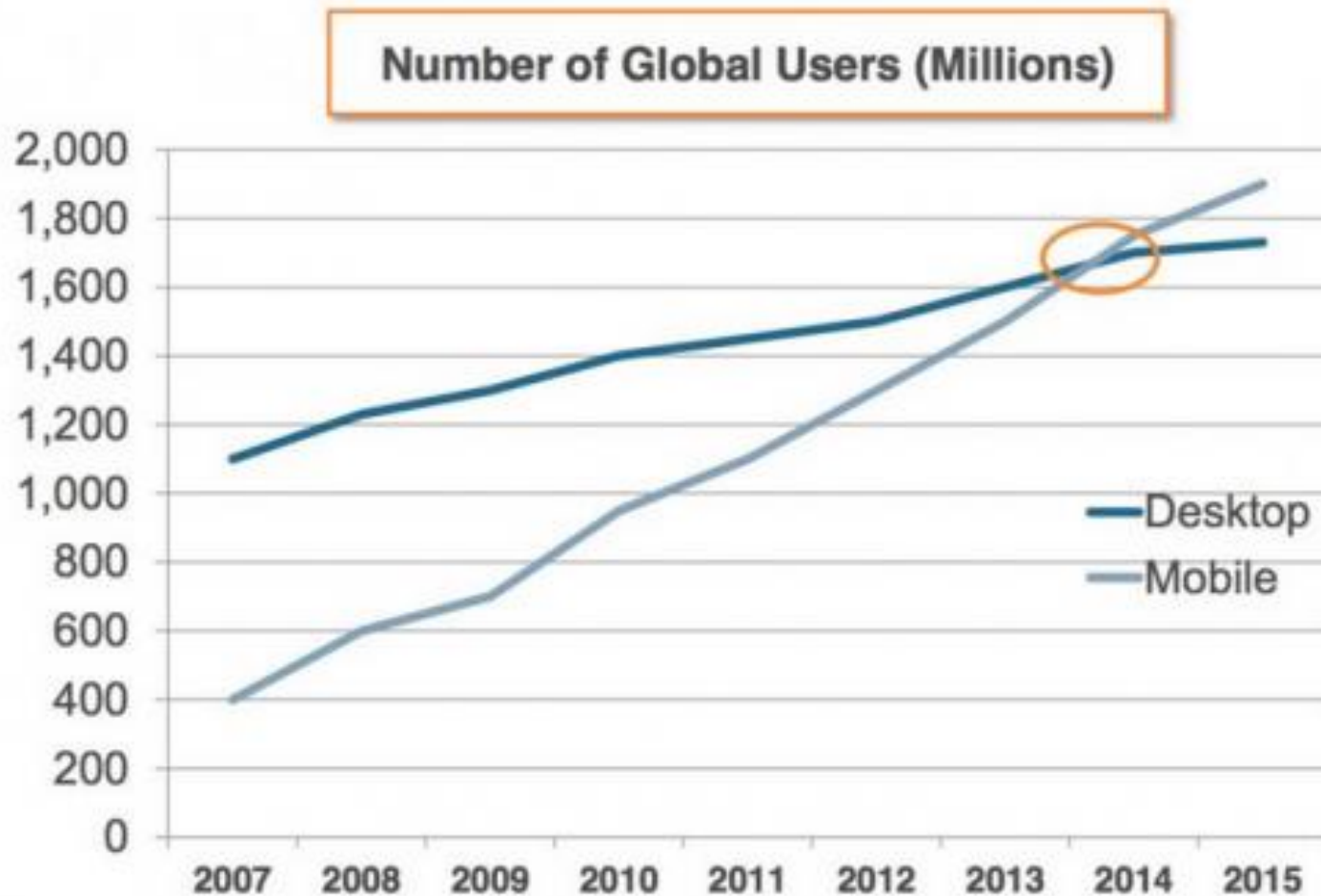
Importancia

- Las aplicaciones móviles son la innovación y el crecimiento de ingreso ya que proporcionan una interacción entre los negocios y sus clientes.
- Las aplicaciones móviles son esenciales para la transformación digital de los negocios ofreciendo un servicio más personalizado a cada uno de sus clientes.



Aplicaciones Móviles

Importancia



El número de usuarios de los dispositivos móviles ha rebasado el número de usuarios de computadoras de escritorio.

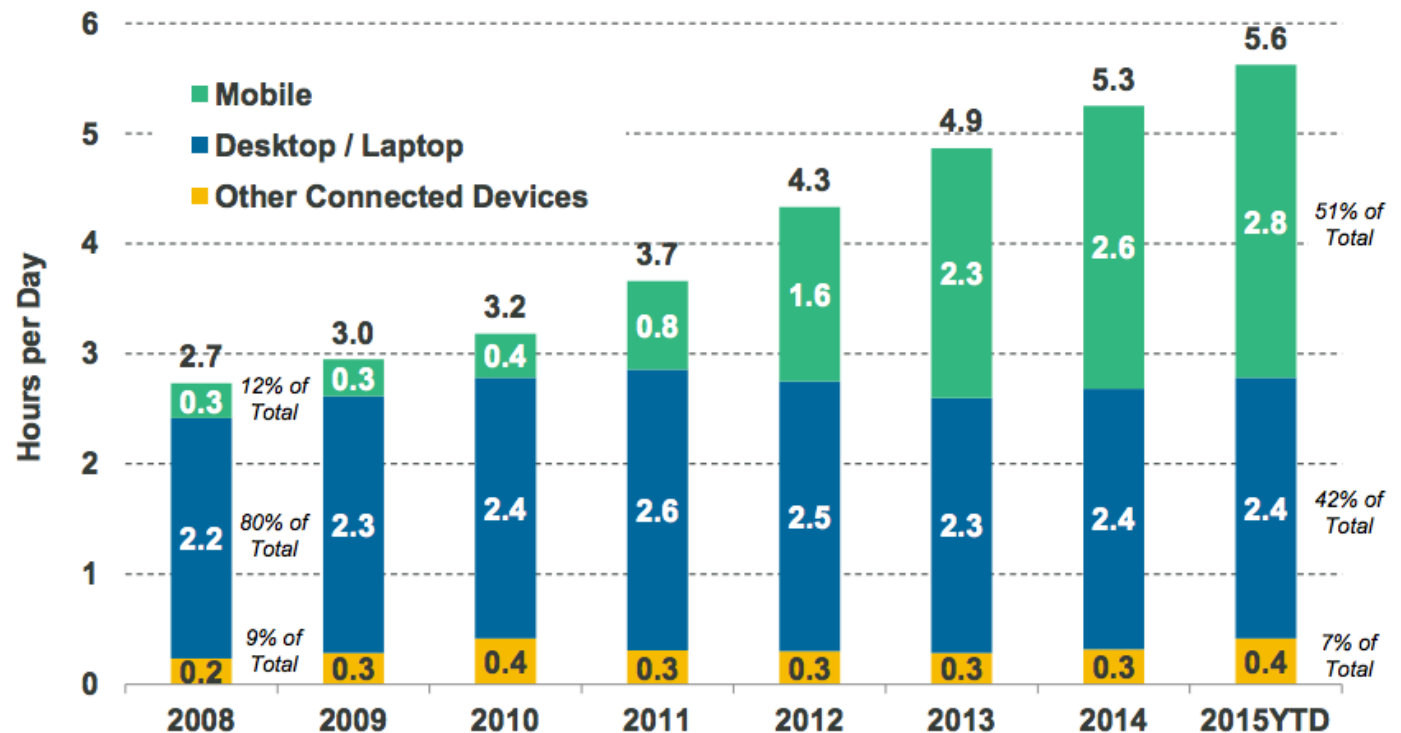
Aplicaciones Móviles

Importancia

Internet Usage (Engagement) Growth Solid
+11% Y/Y = Mobile @ 3 Hours / Day per User vs. <1 Five Years Ago, USA

Los usuarios usan más los dispositivos móviles para consultar el contenido digital.

Time Spent per Adult User per Day with Digital Media, USA, 2008 – 2015YTD



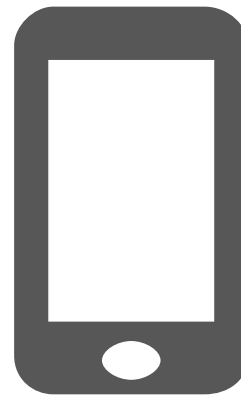
- Las aplicaciones móviles están expuestas a diversas vulnerabilidades que podrían comprometer la confidencialidad, integridad o disponibilidad de la información de las organizaciones y usuarios finales.
- El área de desarrollo de aplicaciones móviles es un espacio nuevo, por lo que las empresas todavía no cuentan con expertos para probar problemas de seguridad y privacidad



Aplicaciones Móviles

Amenazas

Eslabón más **débil** de la seguridad de las empresas son los dispositivos móviles seguido por las redes sociales (Cyber Edge Group)



El **75%** de las aplicaciones móviles no cumplen con los requerimientos básicos de seguridad (Gartner)

Kaspersky Lab detectó 1,363,549 ataques únicos durante 2014. En comparación con 335,000 ataques únicos durante el 2013 hubo un **incremento de 407%**

1 de cada **5** usuarios de Android han experimentado una amenaza móvil en 2014 (Kaspersky Lab)

Propuesta

- Realizar pruebas de seguridad basadas en mejores prácticas y metodologías enfocadas en tecnologías móviles con el fin de analizar:
 - ✓ Código
 - ✓ Diseño
 - ✓ Empaquetamiento
 - ✓ Cifrado
 - ✓ Instalación
 - ✓ Ejecución en diferentes condiciones en las que podría estar sujeto la aplicación.



Caso Real

Aplicación Móvil en
Android

Caso Real

Introducción

- Como parte de los servicios ofrecidos por Deloitte, el equipo realizó una revisión sobre una aplicación móvil para los clientes de esta organización..
- Esta aplicación recibe información altamente confidencial de los usuarios para funcionar



Caso Real

Aplicación

- Como parte de set de pruebas generado para la revisión de esta aplicación, se validaron los controles (OWASP TOP 10)* mediante el análisis a través de ingeniería inversa a la aplicación. Esta fue descompilada y pudimos observar diversos recursos de la aplicación.



Name	Compressed	Original	Type
assets			
lib			
META-INF			
org			
res			
AndroidManifest.xml			
classes.dex			
LICENSE-2.0.txt			
resources.arsc			

*Para más información consultar <https://www.owasp.org/>

Figura 1. Estructura de APK en Android

Caso Real

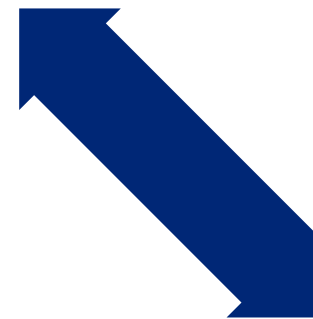
Ingeniería inversa



JAVA

Lenguaje de Alto Nivel

Fácil de Leer y
Escribir



SMALI

Lenguaje de Bajo Nivel

Se puede re-empaquetar
como APK

Análisis de código

- Para la validación se decidió realizar una prueba de inserción de código a la aplicación. De esta forma un atacante puede modificar el flujo lógico de la aplicación para lograr su objetivo.

```
70
71 protected void onCreate(Bundle paramBundle)
72 {
73     super.onCreate(paramBundle);
74
75     setContentView(2130968611);
76     A();
77     if (new com.██████████ a(getApplicationContext()).a())
78     {
79         new com.██████████.ui.b.a().a(getString(2131230821)).b(getString(2131230879)).
80         c(getString(2131230801), "TAG_DIALOG_ROOTED_DEVICE");
81         this.a = false;
82     }
83     while (GooglePlayServicesUtil.isGooglePlayServicesAvailable(this) == 0) {
84         return;
85     }
86     a(new e(), "TAG_DIALOG_PLAY_SERVICE");
87     this.a = false;
88 }
89 protected boolean w()
90 {
91     return this.a;
92 }
93
```

Figure 3. Main Activity – Decompilado a un lenguaje que es human readable

Modificación de código

- La inserción de código se realiza en un lenguaje de bajo nivel y se vuelve a empaquetar como la aplicación original.

```
164
165 .method protected onCreate(Landroid/os/Bundle;)V
166   .locals 3
167   .param p1, "savedInstanceState"    # Landroid/os/Bundle;
168
169   .prologue
170   const/4 v2, 0x0
171
172   invoke-super {p0, p1}, Lcom/██████████/ui/activity/BaseActivity; -> onCreate(
   Landroid/os/Bundle;)V
173
174   const v0, 0x7f040023
175
176   invoke-virtual {p0, v0}, Lcom/██████████/ui/activity/SplashActivity; ->
   setContentView(I)V
177
178   invoke-direct {p0}, Lcom/██████████/ui/activity/SplashActivity; -> A()V
179
180   new-instance v0, Lcom/██████████/mobileclientutilities/a;
181
182   invoke-virtual {p0}, Lcom/██████████/ui/activity/SplashActivity; ->
   getApplicationContext()Landroid/content/Context;
183
184   move-result-object v1
185
186   invoke-direct {v0, v1}, Lcom/██████████/mobileclientutilities/a; -> <init>(Landroid/content
   /Context;)V
187
188   invoke-virtual {v0}, Lcom/██████████/mobileclientutilities/a; -> a()Z
189
190   move-result v0
191
```

Figure 4. Main Activity – Decompilado a un lenguaje bajo nivel

Caso Real

Riesgo

- Debido a esta vulnerabilidad se encontró que la aplicación está expuesta a:
 - ❖ Robo de información confidencial de clientes
 - ❖ Ataques de phishing causando daño reputacional a la organización



Conclusiones

Punto de vista de
seguridad

Conclusiones

Punto de vista de seguridad

- Las tecnologías y desarrollos móviles están creciendo día a día y ofrecen a usuarios y organizaciones una gran cantidad de ventajas para la realización de sus actividades de forma cómoda y ágil.
- Sin embargo, éstas aplicaciones contienen información confidencial y de negocio que puede ser comprometida si no se cuenta con desarrollos robustos y alineados a prácticas de seguridad que permitan disminuir los riesgos de forma considerable





Deloitte se refiere a Deloitte Touche Tohmatsu Limited, sociedad privada de responsabilidad limitada en el Reino Unido, y a su red de firmas miembro, cada una de ellas como una entidad legal única e independiente. Conozca en www.deloitte.com/mx/conozcanos la descripción detallada de la estructura legal de Deloitte Touche Tohmatsu Limited y sus firmas miembro.

Deloitte presta servicios profesionales de auditoría, impuestos, consultoría y asesoría financiera, a clientes públicos y privados de diversas industrias. Con una red global de firmas miembro en más de 150 países, Deloitte brinda capacidades de clase mundial y servicio de alta calidad a sus clientes, aportando la experiencia necesaria para hacer frente a los retos más complejos de los negocios. Cuenta con alrededor de 200,000 profesionales, todos comprometidos a ser el modelo de excelencia.

Tal y como se usa en este documento, “Deloitte” significa Galaz, Yamazaki, Ruiz Urquiza, S.C., la cual tiene el derecho legal exclusivo de involucrarse en, y limita sus negocios a, la prestación de servicios de auditoría, consultoría fiscal, asesoría financiera y otros servicios profesionales en México, bajo el nombre de “Deloitte”.

Esta publicación sólo contiene información general y ni Deloitte Touche Tohmatsu Limited, ni sus firmas miembro, ni ninguna de sus respectivas afiliadas (en conjunto la “Red Deloitte”), presta asesoría o servicios por medio de esta publicación. Antes de tomar cualquier decisión o medida que pueda afectar sus finanzas o negocio, debe consultar a un asesor profesional calificado. Ninguna entidad de la Red Deloitte, será responsable de pérdidas que pudiera sufrir cualquier persona o entidad que consulte esta publicación.