In-seguridad y malware en dispositivos móviles

Damián Muraña

damian @ murana.uy

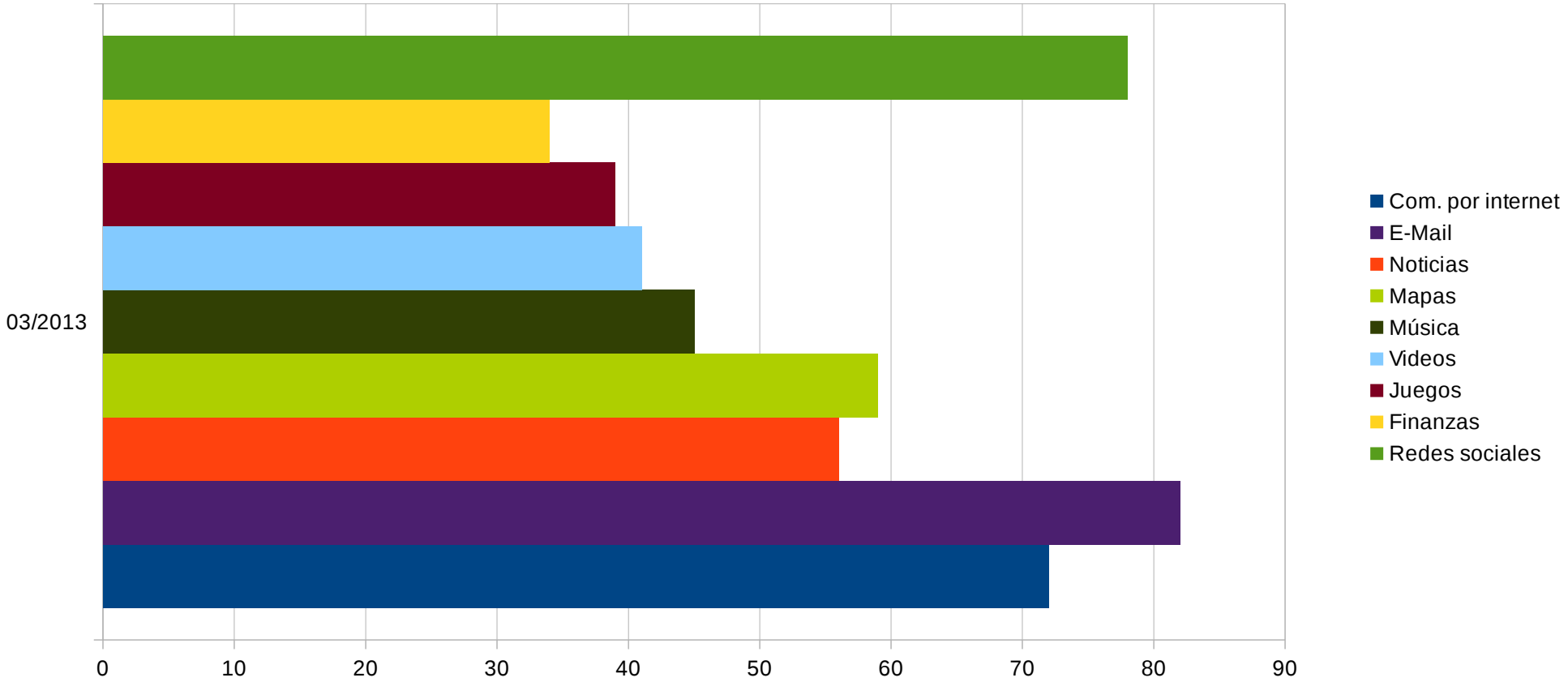
@damianmurana

damianmurana@joindiaspora.com

www.murana.uy

OWASP
The Open Web Application Security Project

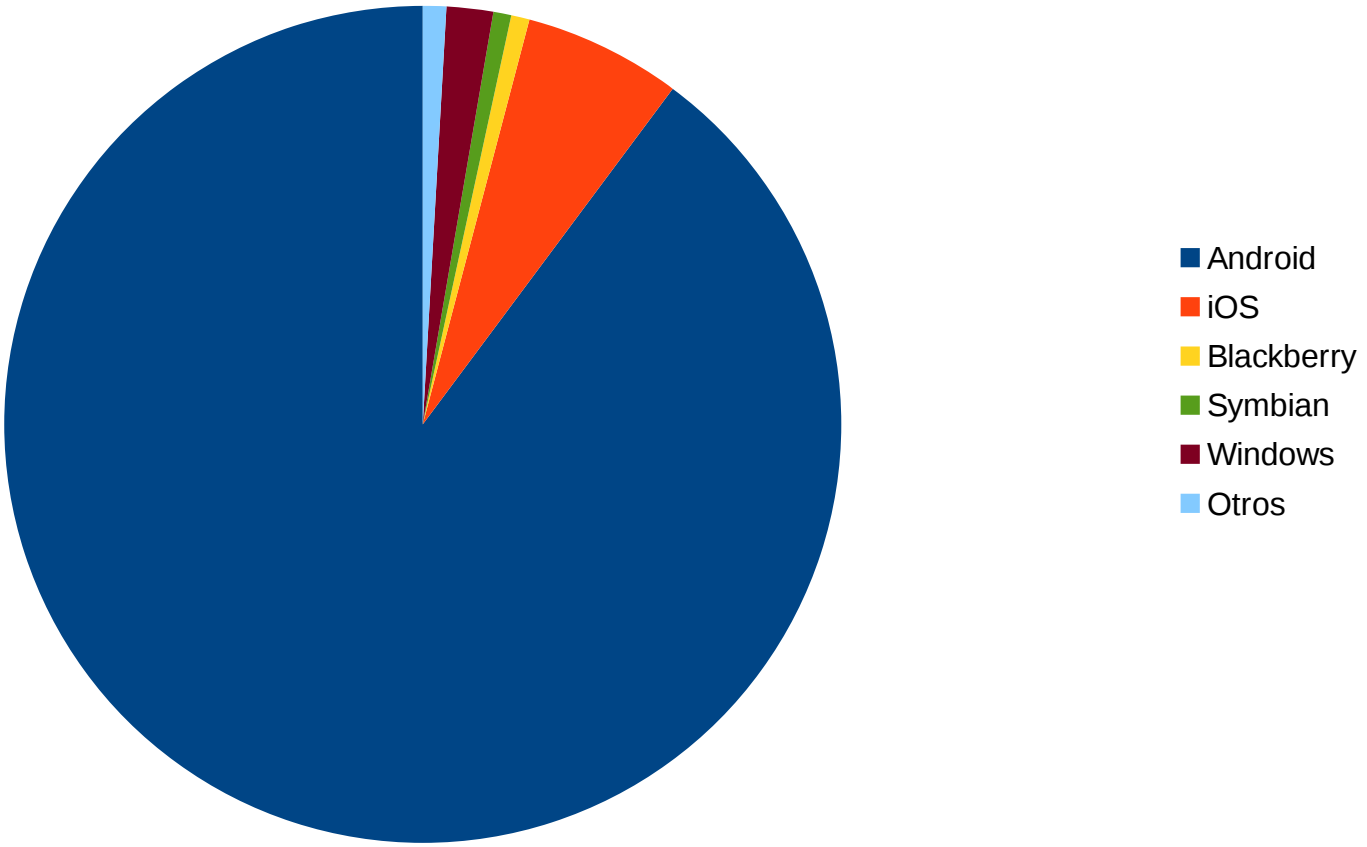
¿Para qué usamos los móviles?



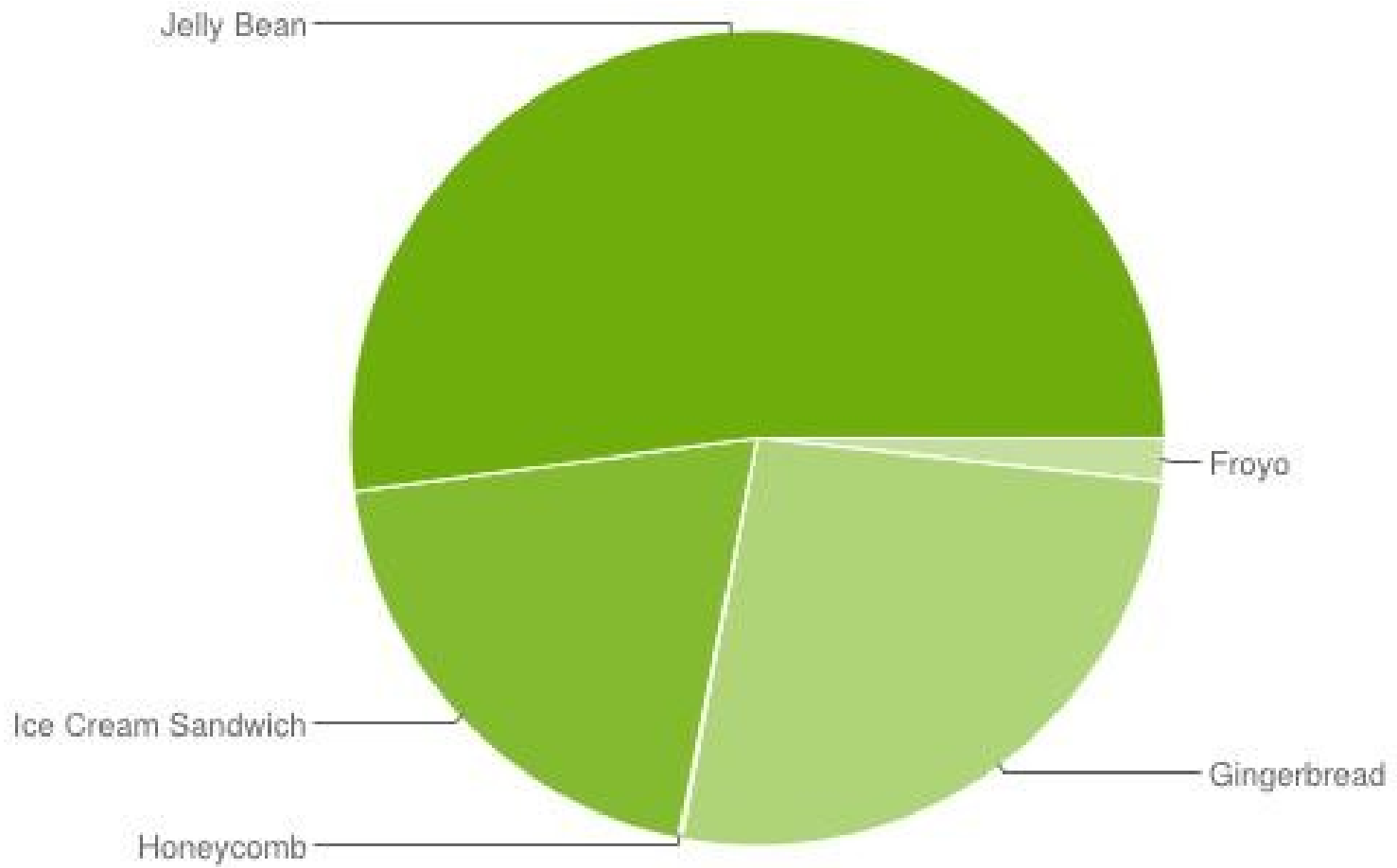
Fuente: The Mobile Movement Study

OWASP
The Open Web Application Security Project

¿Qué plataformas usamos?



Informe IDC. España. Julio 2013.



Actualizado a Febrero 2013.

ANDROID e iOS
¿Qué ha mejorado?

ANDROID

- Nivel de seguridad por defecto más elevado
- Más herramientas de cifrado en versiones ≥ ICS
- Nuevas opciones de desarrollo/depuración
- Google Play Services & Administrador de dispositivos
- Gestor de permisos avanzado (Android 4.3)
- Mejoras en la confianza a desarrolladores

iOS

- Aislamiento entre aplicaciones
- Canales cifrados por y para el ecosistema Apple
- Control estricto en AppStore
- TouchID

¿Qué debemos considerar?

- Las plataformas móviles tienen una evolución muy dinámica, actualizarse es fundamental
- Las aplicaciones móviles se parecen solamente a aplicaciones móviles, la plataformas y los patrones de uso son diferentes a otras
- La aplicación no está aislada, existe un ecosistema a considerar:

  Sistema operativo (y sus fallas de seguridad)

  Integración con la nube y servicios remotos

  Movilidad del dispositivo

  Malware

OWASP Mobile Top 10

- Pensado para ser independiente de la plataforma
- Enfocado en áreas de riesgo en lugar de vulnerabilidades individuales
- Construido usando la OWASP Risk Rating Methodology

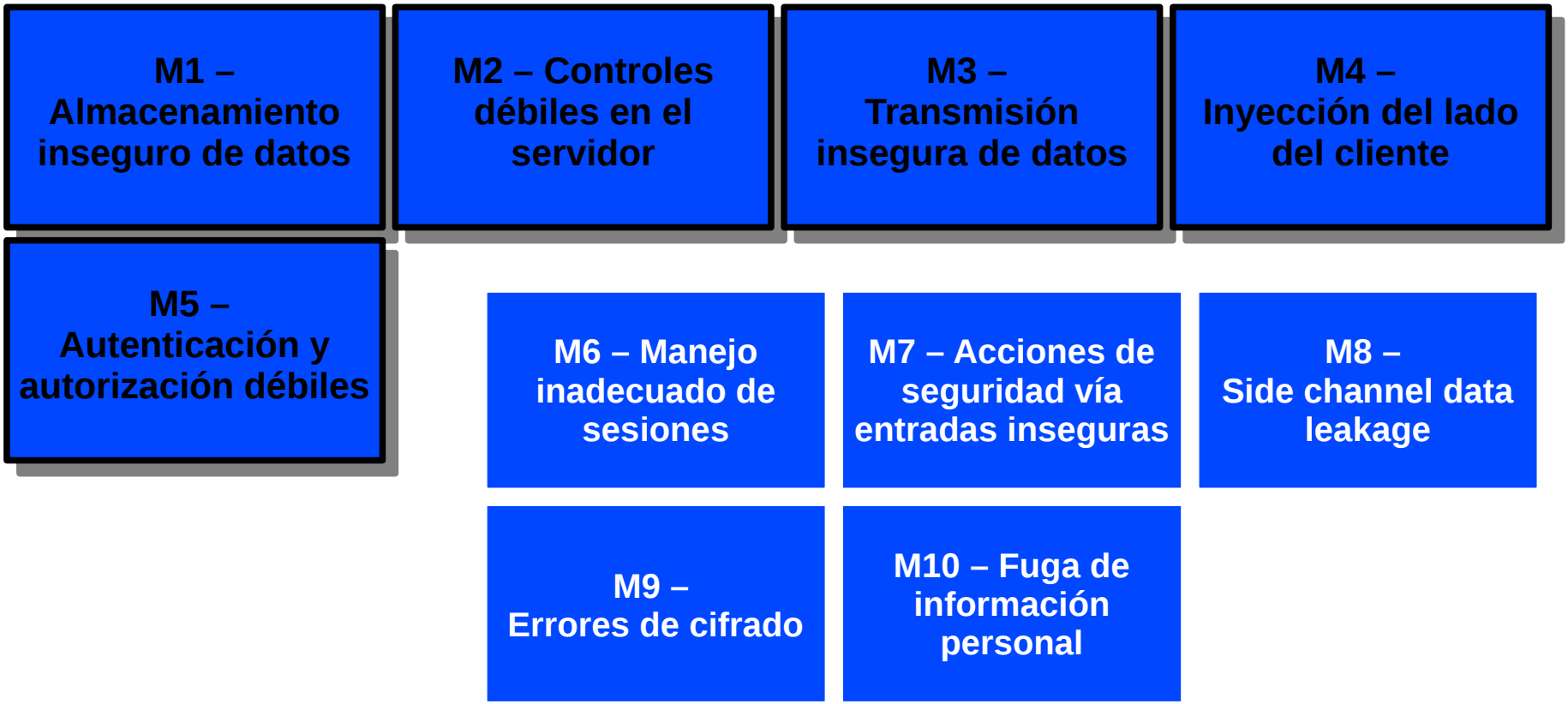
http://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology#The_OWASP_Risk_Rating_Methodology

OWASP Mobile Top Ten 2013

M1 – Almacenamiento inseguro de datos	M2 – Controles débiles en el servidor	M3 – Transmisión insegura de datos	M4 – Inyección del lado del cliente
M5 – Autenticación y autorización débiles	M6 – Manejo inadecuado de sesiones	M7 – Acciones de seguridad vía entradas inseguras	M8 – Side channel data leakage
	M9 – Errores de cifrado	M10 – Fuga de información personal	

OWASP
The Open Web Application Security Project

OWASP Mobile Top Ten 2013



OWASP
The Open Web Application Security Project

M1 – Almacenamiento inseguro de datos

M10 – Fuga de información personal

- Almacenamos mucha información:
  - Archivos (Fotos, Documentos, etc.)
  - Credenciales (Email, Facebook, Twitter, etc.)
  - Correo electrónico, adjuntos y metadatos
  - Cookies
  - Caché del navegador
  - **Geolocalización**
  - **Datos personales y tarjetas de crédito**
  - **Datos telefónicos**
  - **Información de búsqueda**

M1 – Almacenamiento inseguro de datos

M10 – Fuga de información personal

- Los problemas:
  - Cifrado nulo o débil (#9)
  - Protocolos de transferencia inseguros (NFC, Bluetooth, Sync, etc.)
  - Facilidad de acceso a los datos
  - La seguridad por defecto puede no ser suficiente
  - Robo, extravío.

M2 – Controles débiles en el servidor

- Inyecciones
- Cross Site Scripting (XSS)
- Cross Site Request Forgery (CSRF)
- Fallas en la restricción de URLs
- Fallas criptográficas
- Etc.

M3 – Transmisión insegura de datos

- Inseguridad en WiFi
- Cifrado nulo en NFC
- Problemas habituales en Bluetooth
- Protocolos no cifrados (HTTP, SMS, GSM, etc.)
- Aplicaciones que no cifran la transmisión de datos con el servidor (Whatsapp, Twitter, Candy Crush, etc.)
- Exceso de confianza en la red celular (Rouge Cell Base)
- El viejo e inseguro conocido, SSL

M4 – Inyección del lado del cliente

- Lo de siempre: las vulnerabilidades en la web (ejecución de código en el navegador)
- Lo nuevo:
  - Códigos QR, NFC, etc.
  - SMS
  - Comunicación e inyecciones In-App
  - WAP Push

M5 – Autenticación y autorización débiles

- Usar valores fijos como parte de la autenticación (IMEI, IMSI, UUID, DevID, etc.)
- Persistencia de datos.

Recomendaciones

- Evitar almacenar información sensible
- Cuidar el dispositivo móvil del acceso no autorizado

  Valor del dispositivo = Precio de costo + Información
- Informarse sobre las opciones de seguridad. Tener siempre un “plan B”
- Precaución al instalar aplicaciones
- Evitar usar aplicaciones inseguras en contextos críticos (Ej: Whatsapp)
- Desarrollar pensando en la seguridad. Usar las guías OWASP y aplicar conocimientos de seguridad referentes a otras plataformas
- Toda seguridad es poca, siempre buscar medidas extras.
- **No podemos confiar demasiado en el móvil, es un arma de doble filo. Pensar siempre lo peor puede ser lo mejor.**

Gracias por asistir.

OWASP
The Open Web Application Security Project