Cómo se hizo:
El bueno, el feo y el malo

Raúl Siles
DinoSec

www.incibe.es

INSTITUTO NACIONAL DE CIBERSEGURIDAD

SPANISH NATIONAL CYBERSECURITY INSTITUTE

cyber camp
CYBERSECURITY EVENT
2015

incibe_

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

https://cybercamp.es

#CyberCamp15

DinoSec

www.dinosec.com
@dinosec

Raúl Siles
raul@dinosec.com

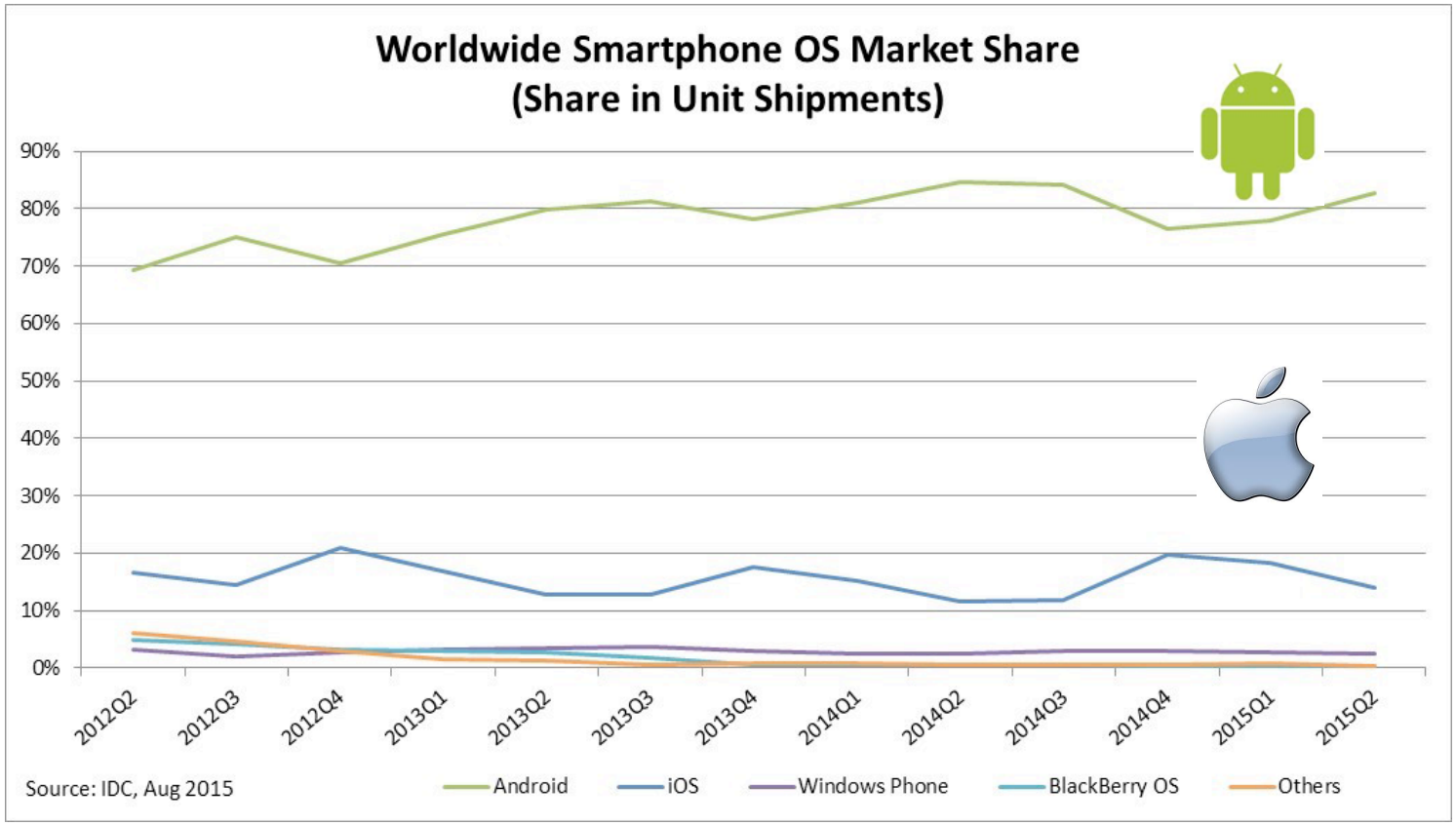
cyber camp

THE GOOD THE BAD AND THE UGLY

El bueno, el feo y el malo

- **Los dispositivos y entornos móviles son un objetivo y están constantemente amenazados por…**
  - Comportamientos del usuario arriesgados…
    - … pero muy habituales
  - Integración con la plataforma del fabricante
    - Apple, Google, Microsoft…
  - Vulnerabilidades de seguridad
    - La importancia de las actualizaciones

Cuota de mercado de los dispositivos móviles



Referencia: http://www.idc.com/prodserv/smartphone-os-market-share.jsp

Q2 2015:

- Android: 82.8%
- iOS: 13.9%
- WP: 2.6%
- BB: 0.3%
- Others: 0.4%

Tendencia consolidada a sobrepasar 300 millones de unidades por trimestre (Qx): 1,3b (2014)

El bueno…

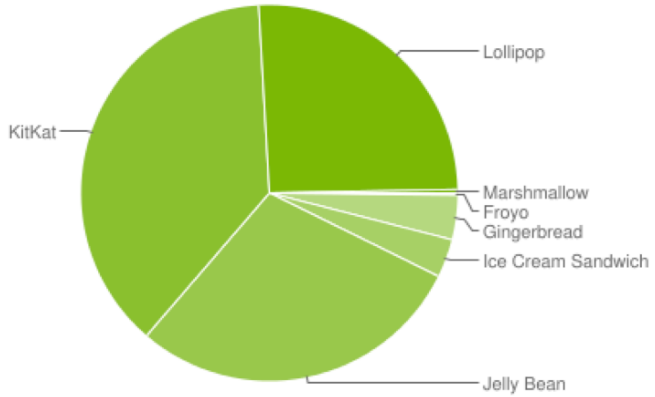
El bueno…

- **¿Disponéis de la última versión del sistema operativo para vuestro dispositivo móvil?**
- **¿Siempre… (tan pronto es publicada)?**
  - Si es que es publicada para vuestro modelo de dispositivo móvil
- **La última versión soluciona todas las vulnerabilidades de seguridad conocidas**
  - ¿Seguro…?
  - ¿…y entre actualizaciones?
  - ¿…y las vulnerabilidades que no son públicas?

Distribución de versiones de Android

- **Noviembre de 2015: https://developer.android.com/about/dashboards/index.html**

Version	Codename	API	Distribution
2.2	Froyo	8	0.2%
2.3.3 - 2.3.7	Gingerbread	10	3.8%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	3.3%
4.1.x	Jelly Bean	16	11.0%
4.2.x		17	13.9%
4.3		18	4.1%
4.4	KitKat	19	37.8%
5.0	Lollipop	21	15.5%
5.1		22	10.1%
6.0	Marshmallow	23	0.3%



Vulnerabilidad Towelroot:

≈ 38%... (≈ 75%)

Data collected during a 7-day period ending on November 2, 2015.

Any versions with less than 0.1% distribution are not shown.

Ritmo al que consumimos la tecnología: Android

- **Android: 8 años**
  - 2008: 1.0
  - 2009: 1.1 & 1.5 & 1.6 & 2.0
  - 2010: 2.1 & 2.2 & 2.3.x
  - 2011: 2.3.x & 3.x & 4.0
  - 2012: 4.1 & 4.2
  - 2013: 4.3 & 4.4
  - 2014: 5.0
  - 2015: 5.1 & 6.0

Nº. oficial de vulnerabilidades:

Desconocido…
(hasta Agosto 2015 para móviles Nexus)

Nº. oficial de vulnerabilidades:

- Ago 15: 6
- Sep 15: 9
- Oct 15: 30
- Nov 15: 7

Android - Total: 52

Ritmo al que consumimos la tecnología: iOS

- **iOS: 9 años**
  - 2007: iPhone 2G (iOS 1)
  - 2008: iPhone 3G (iOS 2)
  - 2009: iPhone 3GS (iOS 3)
  - 2010: iPhone 4 (iOS 4) + iPad 1
  - 2011: iPhone 4S (iOS 5) + iPad 2
  - 2012: iPhone 5 (iOS 6) + iPad 3 & 4 & mini
  - 2013: iPhone 5c & 5s (iOS 7) + iPad air & mini 2
  - 2014: iPhone 6 & 6+ (iOS 8) + iPad air 2 & mini 3
  - 2015: Apple Watch (1 & 2) & iOS 9

Nº. oficial de vulnerabilidades:

- iOS 6: 197
- iOS 7: 80
- iOS 7.1: 41
- …

Nº. oficial de vulnerabilidades:

- iOS 8: 56
- iOS 8.1: 5
- iOS 8.1.1: 9
- iOS 8.1.2: -
- iOS 8.1.3: 34
- iOS 8.2: 6
- iOS 8.3: 58
- iOS 8.4: 33
- iOS 8.4.1: 71

iOS 8.x: 272

Nº. oficial de vulnerabilidades:

- iOS 9: 101
- iOS 9.0.1: -
- iOS 9.0.2: 1
- iOS 9.1: 49

iOS 9.x: 151

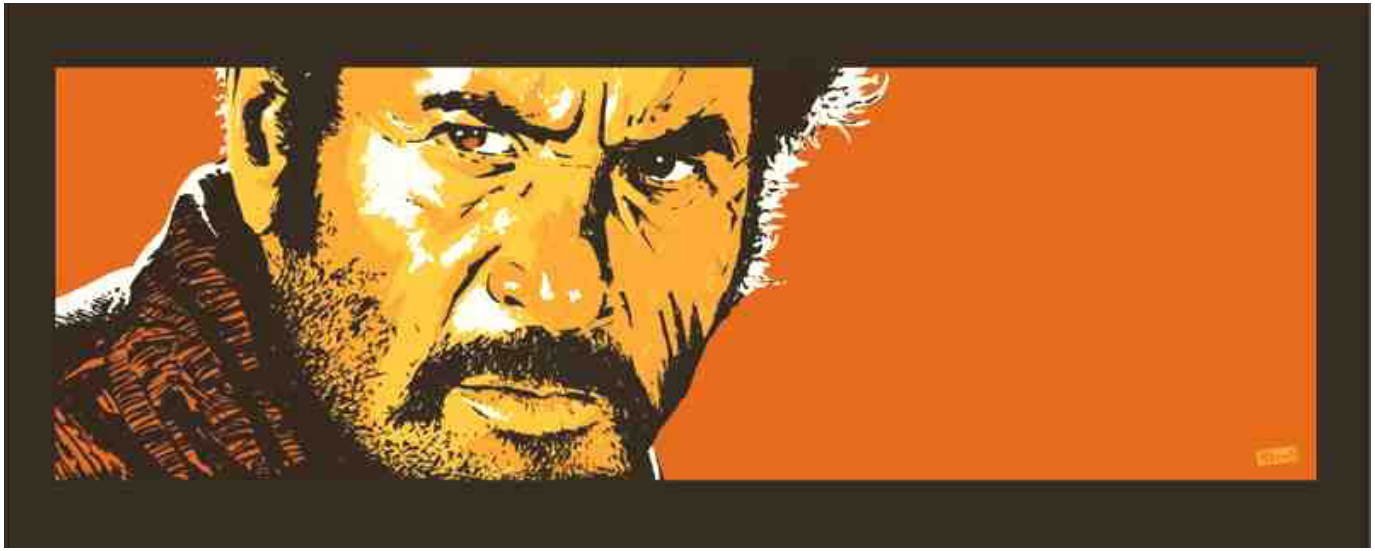
cyber camp

El feo…

El feo…

- **¿Tenéis cuenta de usuario en la plataforma del fabricante del dispositivo móvil?**
  - Apple, Google, Microsoft, etc
- **¿Cuándo la creásteis?**
  - Proceso de instalación y ¿compras?
- **¿Vuestro usuario es conocido?**
  - E-mail
- **La contraseña es robusta, ¿verdad?**
  - Y no la reutilizáis entre distintos servicios…

… el malo

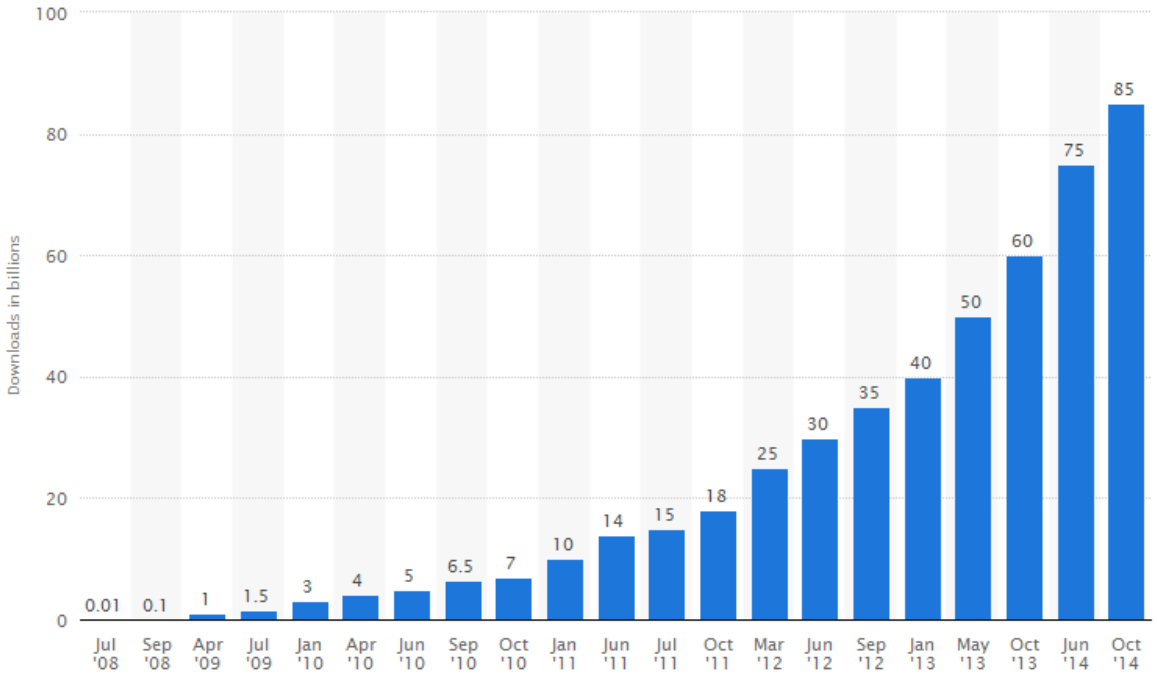


… el malo

- **¿Qué hace que los teléfonos móviles actuales sean inteligentes: *smartphones*?**
- **¿Instaláis aplicaciones móviles (apps) en vuestros dispositivos móviles?**
- **¿Para qué…? (uso profesional, personal…)**
- **¿De quién…? (terceros)**
  - Mercados (oficiales, 3os…) & desarrolladores
- **¿Con qué criterio…? (reputación)**

Mercados oficiales de apps

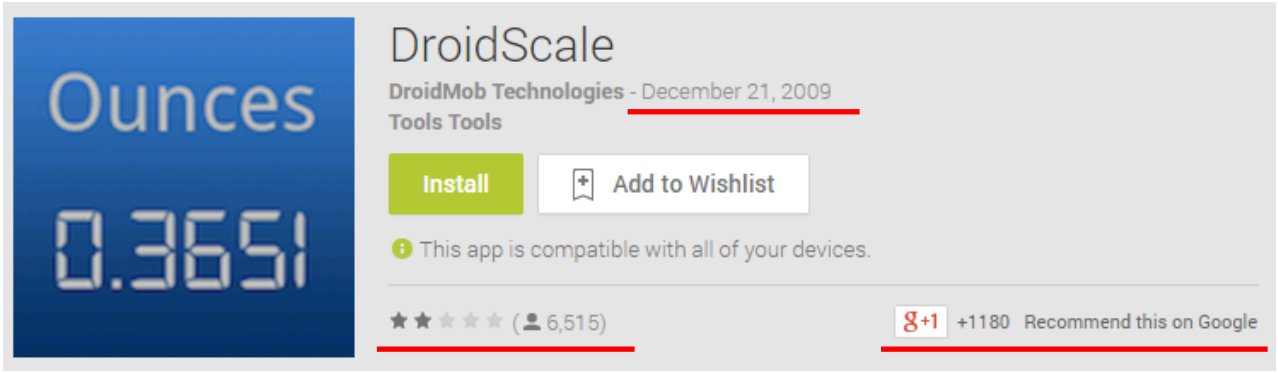
- **App Store, Google Play, etc**
  - 2015:
  - ¿1,5 millones?
  - ¿100,000 millones?



“Malware” móvil: DroidScale

cyber camp

DroidScale (1/3)



Description

OVER 1 MILLION DOWNLOADS!!!!! AD FREE PRO VERSION ALSO AVAILABLE!
This dynamic app turns your phone into a digital scale that you can take with you wherever you go!
Weigh normal household items with your friends, and see who can get the closest guess! Weighs in grams or ounces!
Follow the in-app instructions for use.
Note: DroidScale does not guarantee exact measurements.

Reviews

1.9

6,515 total

5	987
4	250
3	328
2	373
1	4,301

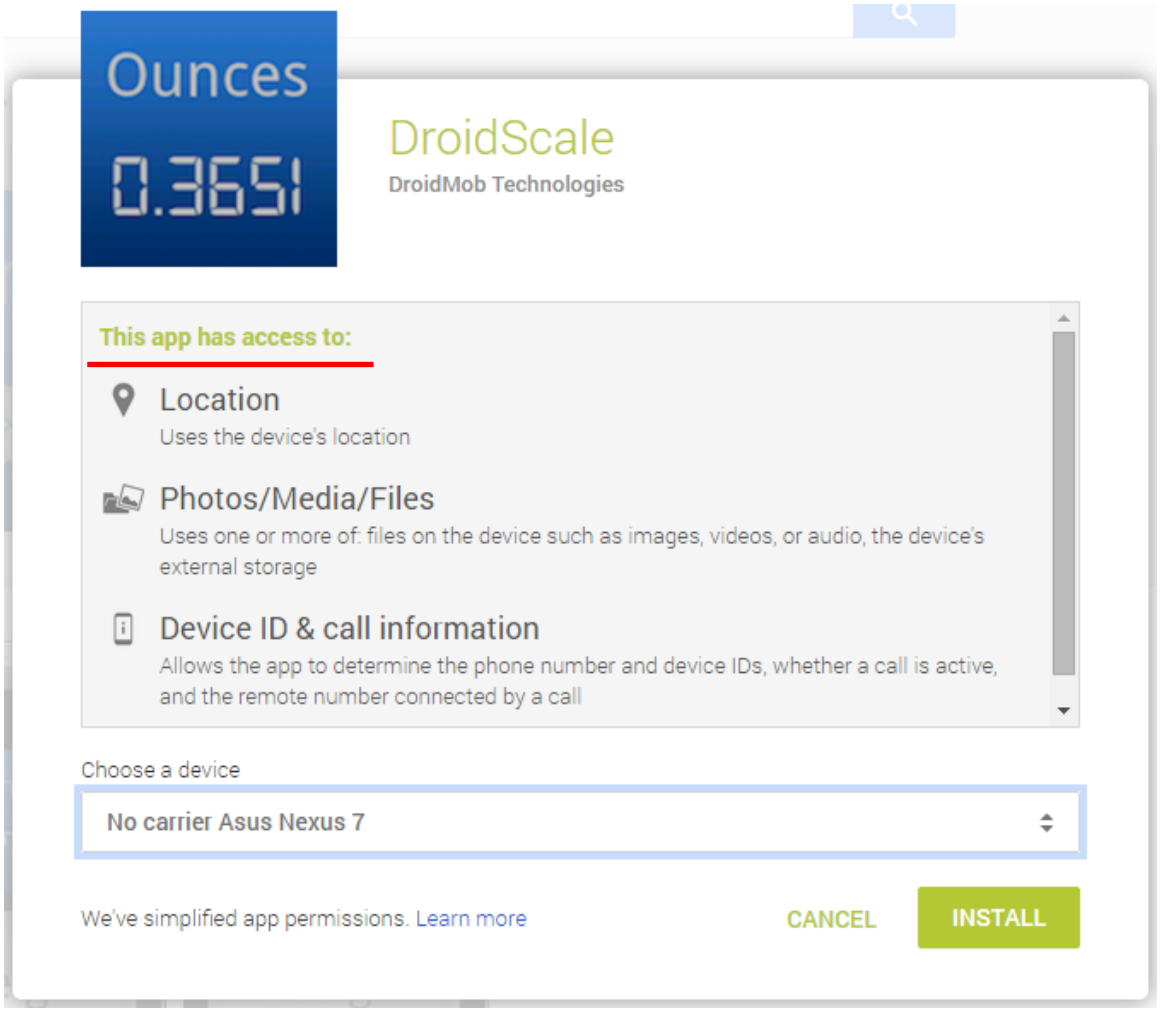
Additional information

Updated	Size	Installs	Current Version	Requires Android	Content Rating
December 21, 2009	155k	1,000,000 - 5,000,000	1.0	1.1 and up	Low Maturity

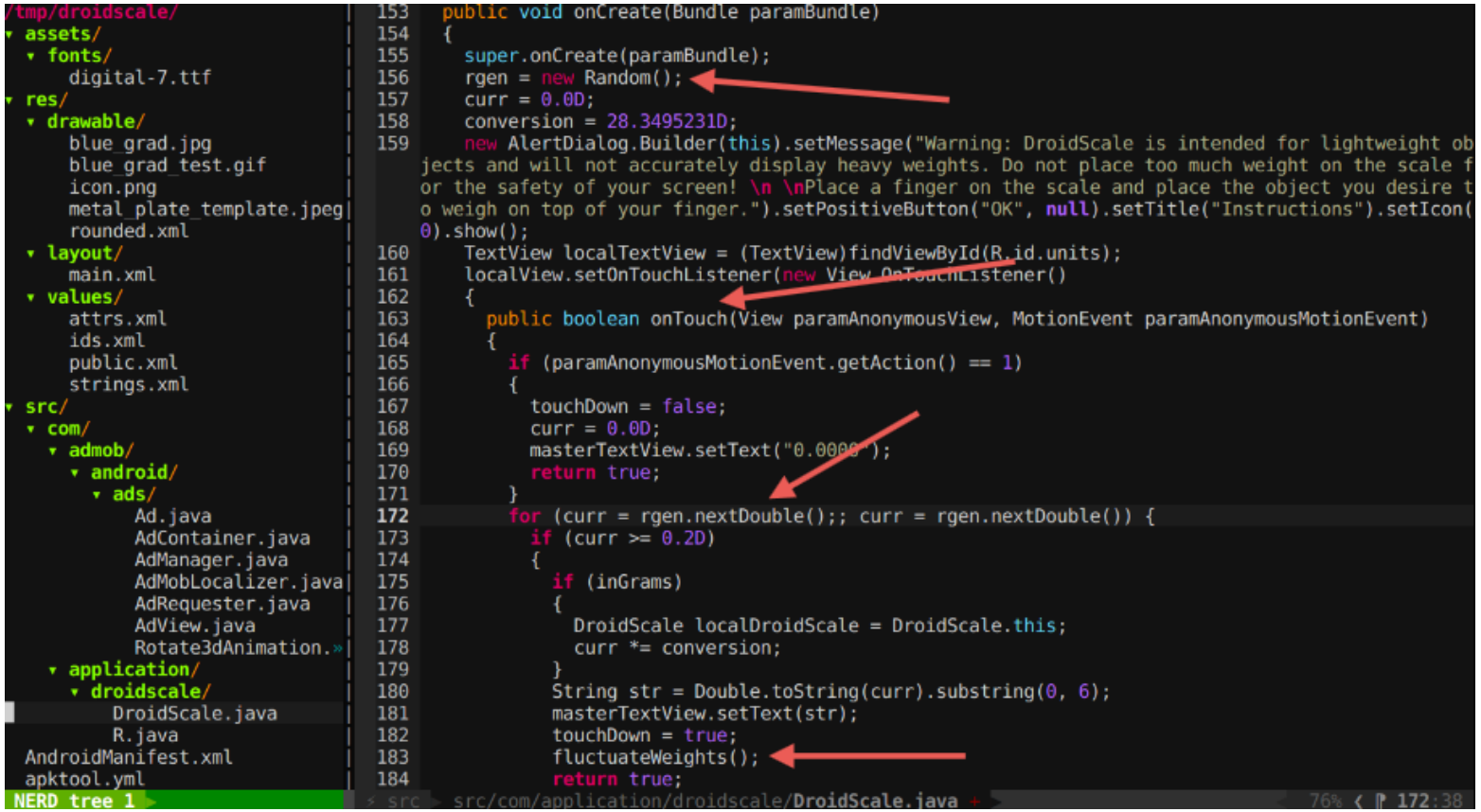
Contact Developer	Permissions	Report
Email Developer	View details	Flag as inappropriate

cyber camp

DroidScale (2/3)



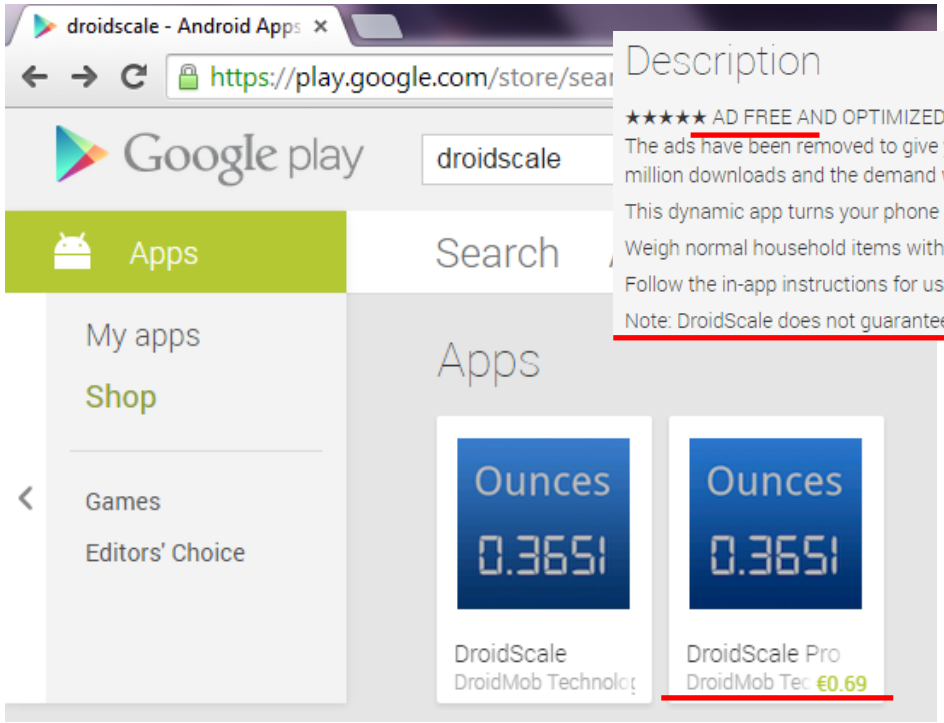
DroidScale (3/3)



Referencia: http://viennot.com/playdrone-slides.pdf

cyber camp

DroidScale Pro (1/2)



Description

★★★★★ AD FREE AND OPTIMIZED! OVER 1 MILLION DOWNLOADS OF THE AD SUPPORTED VERSION! REDUCED INTRODUCTORY PRICE! ★★★★★
The ads have been removed to give you a better experience with more available screen space to weigh your items! The previous ad supported version had over a million downloads and the demand was growing, so the application has been upgraded and optimized in order to give you a better experience!

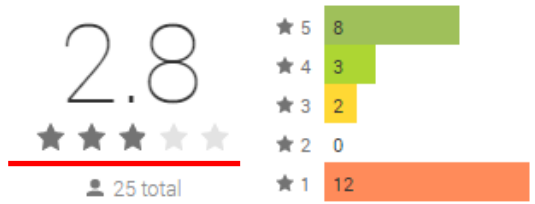
This dynamic app turns your phone into a digital scale that you can take with you wherever you go!

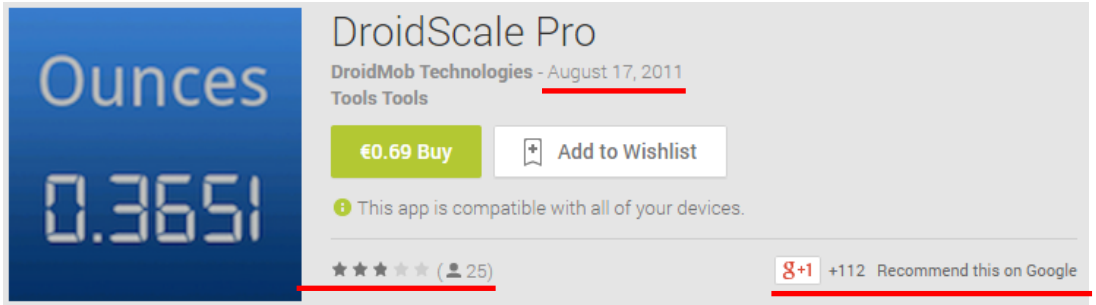
Weigh normal household items with your friends, and see who can get the closest guess! Weighs in grams or ounces!

Follow the in-app instructions for use.

Note: DroidScale does not guarantee exact measurements.

Reviews





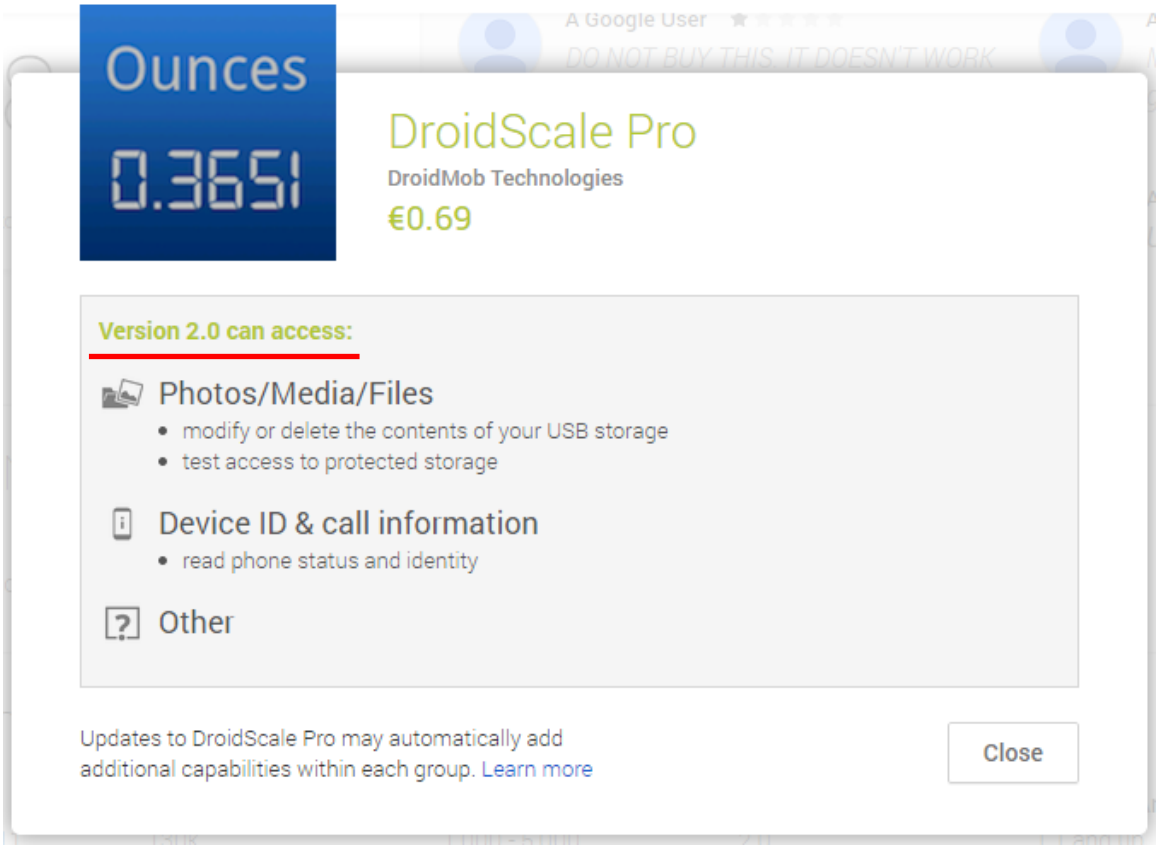
Installs
1,000 - 5,000

Current Version
2.0

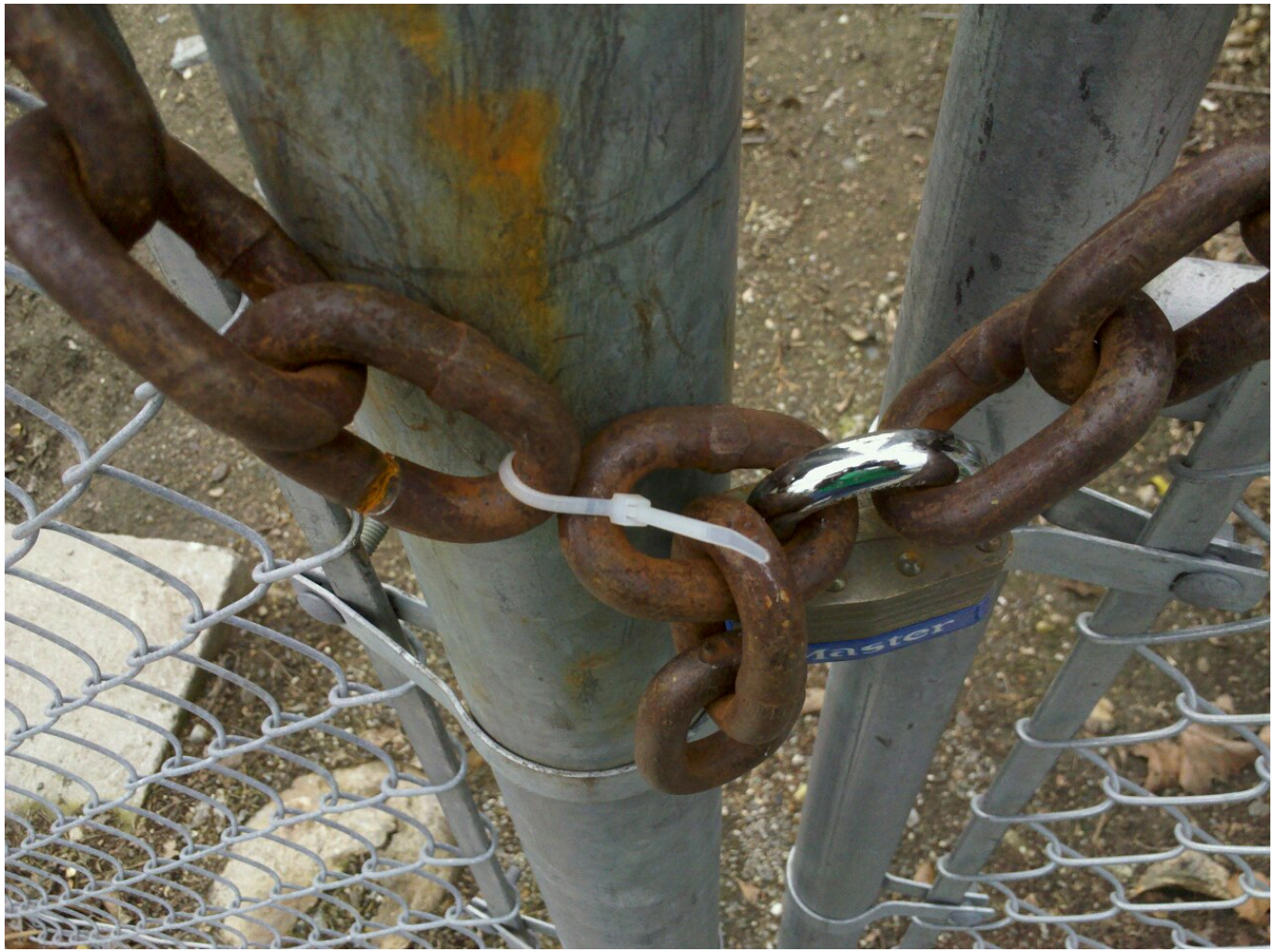
Report
Flag as inappropriate

cyber camp

DroidScale Pro (2/2)



¡Error!



¿Debemos proteger al móvil del usuario?

This is the watermark of FAILKING.COM

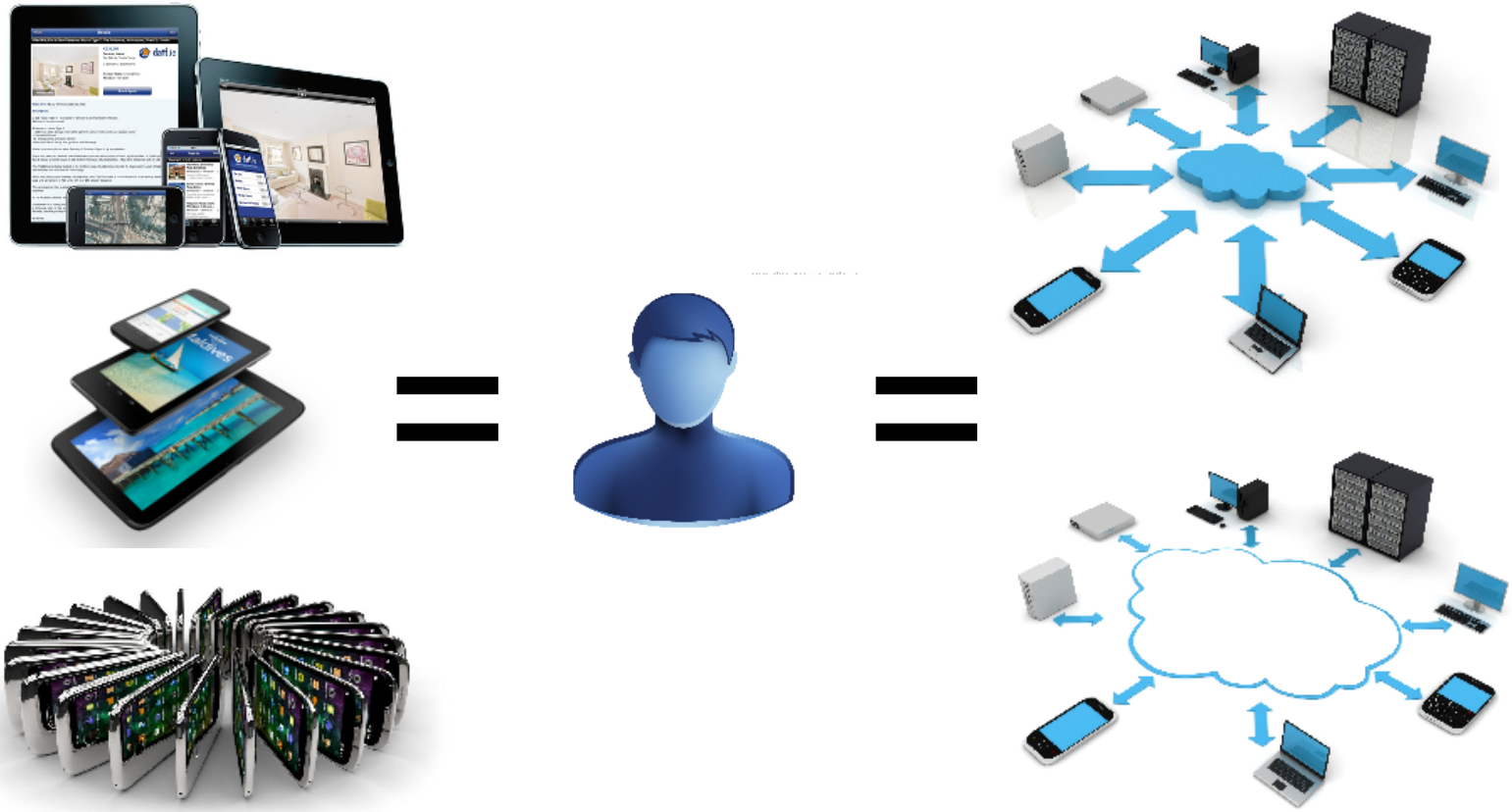
Y U NO go to FAILKING.COM

cyber camp

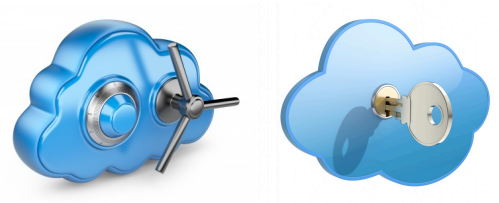
Conclusiones

Protege tu vida digital

- **Dispositivos móviles = Cuenta usuario (credenciales) = Usuario (datos…)**



Riesgo de seguridad móviles



- **Exfiltración de datos e información confidencial**
  - Contenida en el dispositivo móvil
    - Documentos, fotos, ficheros descargados, correos, SMS, registro de llamadas, contactos, geolocalización, WhatsApp y mensajería, redes sociales (privadas)…
    - Contraseña(s) de la red(es) Wi-Fi, código de acceso, patrón de desbloqueo, (gestor de) contraseñas…
  - Credenciales…de acceso a múltiples servicios
    - Internet, "en la nube", VPN, casa, red interna de la organización…
      - E-mail, aplicaciones web, servicios de almacenamiento de ficheros…
  - Ransomware: exfiltración + extorsión, chantaje, DoS…

Recomendaciones

- **Instalar aplicaciones móviles (apps) sólo de los mercados oficiales**
  - Google Play (Android), App Store (iOS), Marketplace (WP)…
    - Verificar su reputación
    - Android: No aceptar apps de "Orígenes desconocidos" (y "Verificar aplicaciones")
- **Selección cuidadosa de las credenciales de usuario: robustas**
- **No realizar el proceso de jailbreak o root**
- **Actualizar los dispositivos móviles a la última versión (…)**
- **Concienciación de los usuarios con menos…**
  - ¿Conocimientos técnicos…? o criterio y experiencia
- **Apps gratuitas: "Si no estás pagando… tú eres el producto"**
- **Implementar una solución de gestión empresarial de dispositivos móviles (*MDM, Mobile Device Management*)**
  - MDM, MAM, MCM… (MEM): Listas blancas de apps verificadas y aprobadas

Preguntas

https://cybercamp.es **#CyberCamp15** **@CyberCampEs**

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD