Deloitte.

Principales riesgos de seguridad en aplicaciones móviles

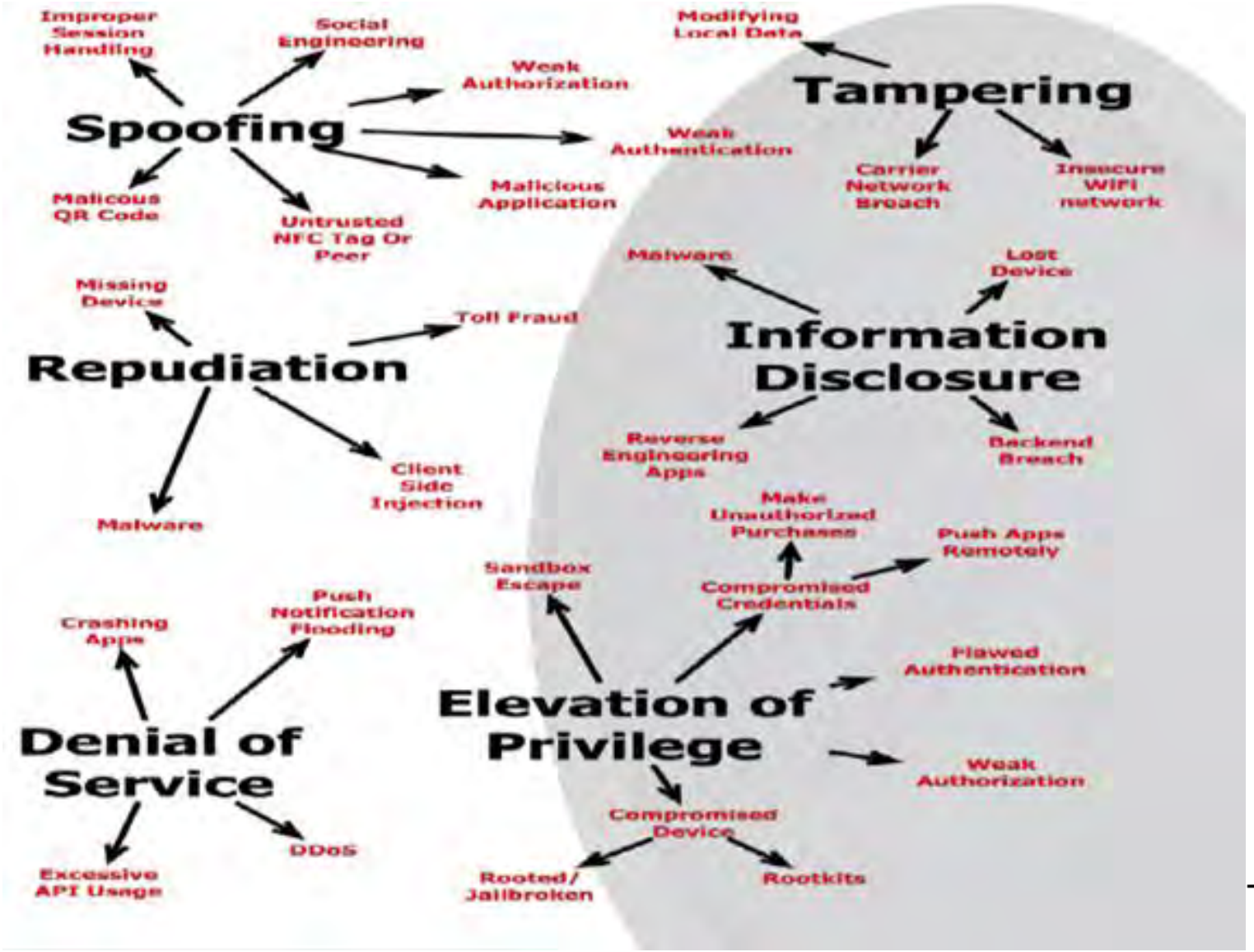
OWASP Mobile Top 10

Mauro Flores

mauflores@deloitte.com
mauro_fcib
DeloitteUySeg

AsIAP
Asociación de Informáticos del Uruguay

Modelo de Amenazas (Threat Model)



©2013 Deloitte Touche Tohmatsu Limited. All rights reserved.

Mobile Top 10

La Lista

1. Almacenamiento Inseguro
2. Errores en controles en el servidor
3. Transmisión insegura de datos
4. Inyección del lado del cliente
5. Autenticación y Autorización débil
6. Manejo Inadecuado de Sesiones
7. Acciones de seguridad vía entradas inseguras
8. Side Channel Data Leakage
9. Errores de Cifrado
10. Fuga de información Personal

jiap 2013

©2013 Deloitte Touche Tohmatsu Limited. All rights reserved.

Mobile Top 10

La Lista

1. Almacenamiento Inseguro
2. Errores en controles en el servidor
3. **Transmisión insegura de datos**
4. Inyección del lado del cliente
5. **Autenticación y Autorización débil**
6. **Manejo Inadecuado de Sesiones**
7. Acciones de seguridad vía entradas inseguras
8. Side Channel Data Leakage
9. Errores de Cifrado
10. Fuga de información Personal

jiap 2013

©2013 Deloitte Touche Tohmatsu Limited. All rights reserved.

Almacenamiento inseguro y Fuga de información

1 2 3 4 5 6 7 8 9 10

¿Qué tipos de datos almacenamos?

- Agenda de contactos y citas
- Fotos personales
- Credenciales de autenticación (mail, Facebook, Twitter, etc)
- Información de trabajo (correos, planillas, documentos, archivos, etc)
- Cookies de sesión
- Archivos temporales de navegación (caché)
- GPS

©2013 Deloitte Touche Tohmatsu Limited. All rights reserved.

Almacenamiento inseguro y Fuga de información

1 2 3 4 5 6 7 8 9 10

¿Cuál es el problema con todo esto ?

- No es común que cifremos los datos
- Otras vulnerabilidades en los distintos protocolos de transferencia usados (Bluetooth, NFC, QR, etc)
- Robo o extravío
- Soporte técnico

©2013 Deloitte Touche Tohmatsu Limited. All rights reserved.

Errores en controles en el servidor

1
2
3
4
5
6
7
8
9
10

http://www.owasp.org/images/4/47/Cloud-Top10-Security-Risks.pdf

OWASP Top 10 – 2010 (New)
A1 – Injection
A2 – Cross Site Scripting (XSS)
A3 – Broken Authentication and Session Management
A4 – Insecure Direct Object References
A5 – Cross Site Request Forgery (CSRF)
A6 – Security Misconfiguration (NEW)
A7 – Failure to Restrict URL Access
A8 – Unvalidated Redirects and Forwards (NEW)
A9 – Insecure Cryptographic Storage
A10 - Insufficient Transport Layer Protection

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

jiap 2013

©2013 Deloitte Touche Tohmatsu Limited. All rights reserved.

Transmisión insegura de datos

1
2
3
4
5
6
7
8
9
10

- Conexión a redes WiFi. Sincronización automática enviando token.
- Algunas aplicaciones móviles, no cifran la comunicación con el server:
  - Twitter
  - Facebook
  - WhatsApp
- Tecnología NFC no cifra, hay que encapsular por SSL
- Ausencia de cifrado en la transmisión de datos (ej: HTTP, SMS, etc)
- Confiar demasiado en la red celular (Rouge Cell Base)
- Ataques al navegador, vulnerabilidad SSL
  - Algoritmos débiles de cifrado
  - Certificados no confiables (ignorando alerta)
  - Ataque a DigiNotar y Comodo

jiap 2013

©2013 Deloitte Touche Tohmatsu Limited. All rights reserved.

Inyección del lado del cliente

1
2
3
4
5
6
7
8
9
10

- Al igual que en el mundo web
  - Ejecución de código en los navegadores

- Nuevas opciones
  - Abuso del tag tel:
  - QR Codes
  - WAP push
  - SMS

©2013 Deloitte Touche Tohmatsu Limited. All rights reserved.

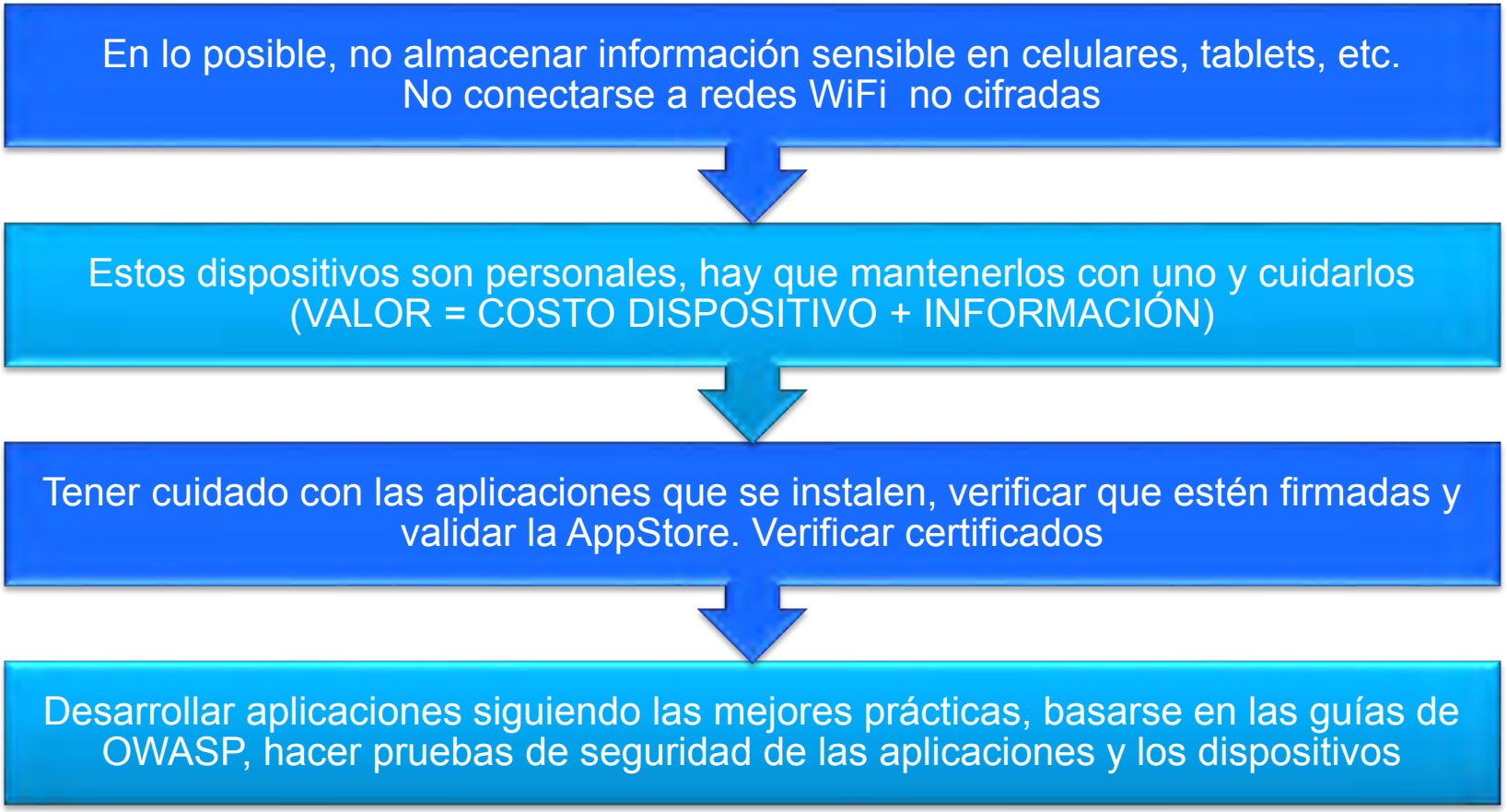
Autenticación débil

1 2 3 4 **5** 6 7 8 9 10

- Depender de valor fijos y que pueden comprometerse (ej: IMEI, IMSI y UUID)
- Identificadores de hardware persisten a los resets
- Out-of-band no es efectiva si todo sale del mismo dispositivo.

©2013 Deloitte Touche Tohmatsu Limited. All rights reserved.

Algunas recomendaciones



©2013 Deloitte Touche Tohmatsu Limited. All rights reserved.

Conclusiones

- A los dispositivos móviles, se les dá mas confianza de la que merecen, cuando debería ser todo lo contrario
- El celular es un ambiente dinámico y como tal hay que incorporar medidas extras de seguridad
- La gente es más propensa a instalar aplicaciones —curiosas”, sin importar su procedencia
- El celular es un punto de acceso a la información de nuestras vidas, y está muy expuesto
- Esta película, ya la vimos…

©2013 Deloitte Touche Tohmatsu Limited. All rights reserved.

Conclusiones

- **… debemos cambiarle el final!**
- Hay que usarlo con conciencia
- Considerar las vulnerabilidades comunes para otras plataformas y trasladar los mecanismos de protección al mundo móvil
- El desarrollo debe considerar medidas extras de seguridad para estos dispositivos

©2013 Deloitte Touche Tohmatsu Limited. All rights reserved.

Links de referencia

Proyecto OWASP

- https://www.owasp.org/index.php/Main_Page

OWASP –Mobile Security Project”:

- https://www.owasp.org/index.php/OWASP_Mobile_Security_Project

NIST – —Guide to bluetooth security”:

- http://csrc.nist.gov/publications/nistpubs/800-121/SP800-121.pdf

NIST – –Cell Phone and PDA Security”

- http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf

©2013 Deloitte Touche Tohmatsu Limited. All rights reserved.

Deloitte.

Mauro Flores

mauflores@deloitte.com
mauro_fcib
DeloitteUySeg