



OWASP Seguridad Para Móviles

Alexandro Fernandez
Security Consultant
Sm4rt Security Services
alexandro@sm4rt.com
55 3520 1675

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the OWASP License.

The OWASP Foundation
<http://www.owasp.org>

OWASP
11 Nov. 2011

Agenda

- Introducción
- Riesgos más comunes
- Vulnerabilidades más comunes
- Mejores Prácticas
- Recomendaciones & Conclusiones

OWASP  2

Agenda

- Introducción
- Riesgos más comunes
- Vulnerabilidades más comunes
- Mejores Prácticas
- Recomendaciones & Conclusiones

OWASP  3

Recordemos...

1990



OWASP  4

Recordemos...

2000



OWASP 5

Sigamos recordando...

2005



OWASP 6

Ya casi...

2007



OWASP 7

Ya llegamos...

2007 a 2010



OWASP 8

Ya estamos aquí...

2011



OWASP 9

Y el futuro...

2025



OWASP 10

ALGUNAS CIFRAS

Sistemas operativos de Smartphones & participación de mercado 2011, y CAGR (listado alfabéticamente) 2011-2015

Sistema Operativo	Participación de Mercado 2011	Participación de Mercado 2015	*CAGR 2011-2015
Android	39.50%	45.40%	23.80%
BlackBerry	14.90%	13.70%	17.10%
iOS	15.70%	15.30%	18.80%
Symbian	20.90%	0.20%	-65.00%
Windows Phone 7/Windows Mobile	5.50%	20.90%	67.10%
Others	3.50%	4.60%	28.00%
Total	100.00%	100.00%	19.60%

Fuente: IDC Worldwide Quarterly Mobile Phone Tracker, Marzo 29, 2011

* CAGR Compound Annual Growth Rate (Tasa de crecimiento en un año de una inversión durante un período de tiempo determinado)

OWASP

Gartner®

Espera un crecimiento en ventas de Smartphones (solo en Estados Unidos) **de 67 millones en 2010 a 95 millones en 2011**

Y se espera llegar a los **500 millones de Smartphones en 2012 !!**

OWASP

Morgan Stanley

Estima que las ventas de Smartphones **superen las ventas de PCs en 2012**

OWASP

Entonces, por qué la seguridad en móviles es tan importante?

OWASP 14

"Attackers are turning to mobile platforms, researcher says"

Mikko Hypponen, Chief Research Officer, F-Secure Corp.

"Security markets are heavily influenced by moving threat-targets in the mobile device space."

John Girard, VP Distinguished Analyst, Gartner

"Google's Android platform is now the most popular for malicious mobile programs, overtaking other platforms as well as 'generic' Java malware."

Warwick Ashford, Chief reporter at Computer Weekly

OWASP 15

HECHOS



- El uso de Smartphones como **herramienta de trabajo** ha alcanzado un punto de inflexión.
- Los teléfonos móviles **superarán a las PCs** como los dispositivos más comunes de acceso a Internet a nivel mundial.
- La situación es que las plataformas de los usuarios de Smartphones **son inherentemente inseguras** y los dispositivos móviles están expuestos a las amenazas de la red.

OWASP

Agenda

- Introducción
- **Riesgos más comunes**
- Vulnerabilidades más comunes
- Mejores Prácticas
- Recomendaciones & Conclusiones

OWASP  17

Riesgos más comunes

Fuga de Datos (Data leakage)

Un Smartphone robado o perdido sin protección, permite a un atacante acceder los datos que en él se contengan.



**Sin
contraseña!!**

OWASP 

Riesgos más comunes

Divulgación no intencional de datos

La mayoría de las aplicaciones tienen opciones de privacidad pero muchos de los usuarios desconocen esto.



OWASP 

Riesgos más comunes

Phishing

Un atacante puede conseguir credenciales del usuario (P.E. contraseñas, números de tarjetas de crédito) usando aplicaciones falsas o enviando mensajes (SMS, correo electrónico) que parecen genuinos.



OWASP 

Riesgos más comunes

Ataques de suplantación (red)

Un atacante despliega un punto de acceso (Access point) a la red y el usuario se conecta. El atacante intercepta la comunicación del usuario para llevar a cabo ataques futuros.

Internet

Starbucks (falso)

SSID: Starbucks
User: Starbucks01
Pw: Chai01

OWASP

Riesgos más comunes

Malware financiero

Diseñado para robar números de tarjetas de crédito, credenciales de banca en línea o afectar transacciones de comercio electrónico.

Ejemplos:

- ▶ ZeuS Mitmo
- ▶ SpyEye
- ▶ Bankpatch
- ▶ Sinowal
- ▶ Gozi.

OWASP

Riesgos más comunes

Ataque de Dialerware

Un atacante puede robar dinero de un usuario por medio de un malware que hace uso (normalmente oculto) de los servicios del Smartphone.

123456789

1 2 3
4 5 6
7 8 9
* #

Options

OWASP

Riesgos más comunes

Spyware

▶ El spyware instalado permite al atacante acceder o inferir datos personales.

▶ Esto incluye cualquier software que pueda estar solicitando y/o haciendo peticiones excesivas de privilegios.

Legítima

Falsa

Steamy Window

Do you want to install this application?

Allow this application to:

- ✓ Network communication
- ✓ Hardware controls
- ✓ Record audio

Hide

Install Cancel

Do you want to install this application?

Allow this application to:

- ✓ Your messages receive SMS
- ✓ Your personal information write to your device and read its data
- ✓ Write Browser's history and bookmarks
- ✓ Network communication full Internet access

Install Cancel

OWASP

Riesgos más comunes

			R1
			R2
Impacto	Altos	Médios	R3
	Médios	Altos	R4
Bajos	Altos	Médios	R5
	Médios	Altos	R6
			R7

- R1 Fuga de Datos
- R2 Divulgación no intencional de datos
- R3 Phishing
- R4 Ataques de suplantación (red)
- R5 Malware Financiero
- R6 Ataques de Diallerware
- R7 Spyware

* Fuente ENISA (European Network and Information Security Agency)

OWASP

Agenda

- Introducción
- Riesgos más comunes
- **Vulnerabilidades más comunes**
- Mejores Prácticas
- Recomendaciones & Conclusiones

OWASP

Vulnerabilidades más comunes

Una débil o inexistente gestión de parches.



OWASP

Vulnerabilidades más comunes

Reportes de vulnerabilidades

National Vulnerability Database

CVE-2011-4774

Summary: Cross-site scripting (XSS) vulnerability in the A-Form PC and PC-Mobile before 3.1 plays its for Movable Type allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, a different vulnerability than CVE-2011-376.

Publish: 11/09/2011

CVSS Severity: 3.9 (HIGH)

CVE-2011-2076

Summary: The A-Form and A-Form bamboo before 1.3.6 and 2.x before 2.0.3, and 4-Form PC and PC-Mobile before 3.1, play its for Movable Type do not require administrative authentication, which allows remote authenticated users to modify data via unspecified vectors.

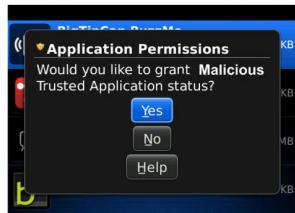
Publish: 11/03/2011

CVSS Severity: 3.9 (HIGH)

OWASP

Vulnerabilidades más comunes

Firmado ≠ confianza



OWASP

Vulnerabilidades más comunes

Ambiente de pruebas pobre o inexistente



OWASP

Vulnerabilidades más comunes

Cifrado débil



OWASP

Agenda

- Introducción
- Riesgos más comunes
- Vulnerabilidades más comunes
- Mejores Prácticas
- Recomendaciones & Conclusiones

OWASP 32

Mejores prácticas - Usuarios



"Mejor enséñame a configurar mi Smartphone, si? "

OWASP 33

Mejores prácticas - Usuarios

Desactivar los servicios inalámbricos si no los esta usando.



OWASP

Mejores prácticas - Usuarios

Mantener la **seguridad física** del dispositivo.



OWASP

Mejores prácticas - Usuarios

Bloquear el dispositivo



OWASP

Mejores prácticas - Usuarios

No almacenar **información confidencial** en estos dispositivos.



OWASP

Mejores prácticas - Usuarios

Reportar cualquier **actividad sospechosa** de su Smartphone.



OWASP

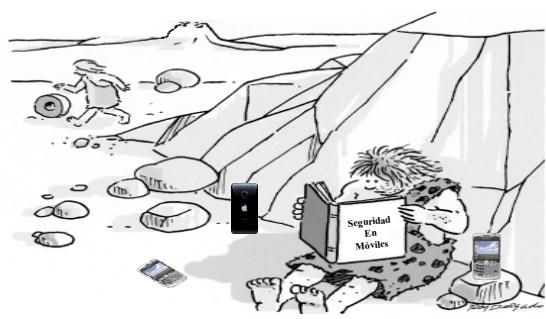
Mejores prácticas - Usuarios

Reportar el equipo en caso de ser robado.



OWASP

Mejores prácticas – Seguridad Informática



OWASP 40

Seguridad Informática

Cifre la información - Algunos **sistemas operativos** para Smartphones o soluciones de gestión, vienen equipadas con la funcionalidad de cifrar información en el Smartphone.



OWASP

Seguridad Informática

Monitoree los dispositivos móviles - Implemente sistemas de monitoreo para el dispositivo móvil.



OWASP

Seguridad Informática

Configurar una línea telefónica (01-800-help-me-please) para reportar el robo de equipos.



OWASP

Seguridad Informática

Borre datos de manera remota – Habilite funcionalidades de borrado remoto para eliminar el contenido del Smartphone que fue robado.



OWASP

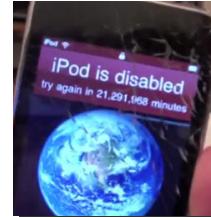
Seguridad Informática

Acceso con contraseña: Habilite la política de contraseñas en el Smartphone.



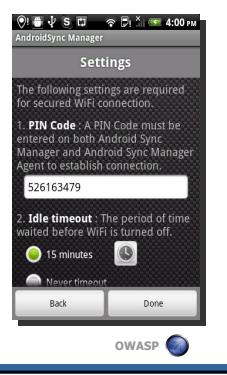
Seguridad Informática

Intentos fallidos en la contraseña: Configure el dispositivo para que realice un borrado seguro de los datos después de un número predefinido de intentos fallidos en la autenticación.



Seguridad Informática

Tiempo de inactividad: Habilite la protección con contraseña de la pantalla cuando se haya llegado a cierto tiempo de inactividad.



Seguridad Informática

Seguridad inalámbrica: Habilite políticas de seguridad para deshabilitar el uso de la WiFi mientras se encuentre conectado a la red del carrier.



Seguridad Informática



Descargas: Elabore, configure y aplique políticas de seguridad en laptops y desktops que controlen las descargas a los Smartphones.



OWASP

OWASP 50

Agenda

- Introducción
- Riesgos más comunes
- Vulnerabilidades más comunes
- Mejores Prácticas
- **Recomendaciones & Conclusiones**

Recomendaciones



"No se preocupe director, en OWASP day
aprendí lo necesario para asegurar los
Smartphones de la empresa"

OWASP

Recomendaciones & Conclusiones

- Los Smartphones son magníficas herramientas de trabajo, sin embargo **el negocio es el responsable final** de autorizar su uso.



OWASP

Recomendaciones & Conclusiones

- Se debe entender el **riesgo del negocio** que representa el uso de estos dispositivos.



- Los riesgos **deben ser evaluados** para asegurar que la información de la empresa esta protegida y disponible en todo momento.

OWASP

Recomendaciones & Conclusiones

- Una vez que los **beneficios y los riesgos son entendidos**, el negocio debe utilizar un **marco de gobierno** que asegure que los cambios en los procesos y en las políticas son implementados y comprendidos.



OWASP

Y finalmente..... Algunas opciones



SOPHOS
Sophos Mobile Control

 **Check Point**
SOFTWARE TECHNOLOGIES LTD.
Pointsec Mobile Security



OWASP

Preguntas?



OWASP

Muchas gracias!



Alexandro Fernández R.

CISSP, CISA, CISM, ISSPC, CEH, ECSA, ISO 27001 LA, COBIT

alexandro@sm4rt.com