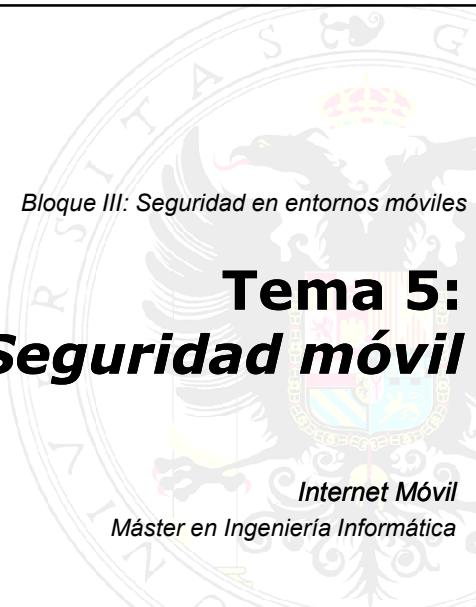


Bloque III: Seguridad en entornos móviles

Tema 5: **Seguridad móvil**



Internet Móvil
Máster en Ingeniería Informática

 Pedro García Teodoro
Dpto. Teoría de la Señal, Telemática y Comunicaciones



Índice



1. Introducción
2. Fundamentos de seguridad
3. Arquitectura AAA
4. Gestión de la seguridad

Internet Móvil - MTI
Tema 5: Seguridad móvil
© PGTe - DTSTC - UGR 2017



1. Introducción (i)

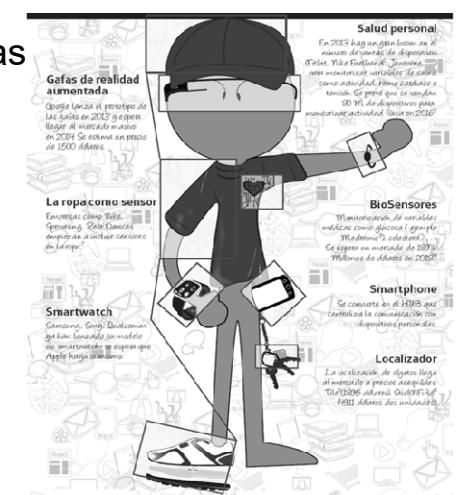
- TIC, base de la e-sociedad
- Necesidad de seguridad:
 - Los clientes deben confiar en la red y los servicios que ésta ofrece
 - Las autoridades exigen un nivel de seguridad mediante normas y leyes, para garantizar la disponibilidad de los servicios, la libre competencia y proteger la privacidad
 - Los operadores y proveedores de servicios necesitan seguridad para salvaguardar su funcionamiento e intereses comerciales y cumplir con sus obligaciones ante los clientes

- ITU-T. "La Seguridad de las Telecomunicaciones y las Tecnologías de la Información", 2006.

3

1. Introducción (ii)

- Complejidad sistemas actuales:



4

1. Introducción (iii)

■ Evolución vulnerabilidades:

Fuente: Cisco, 2014

5

Internet Móvil - MIT
Tema 5: Seguridad móvil
© PGIT - DTSTC - UGR - 2017

DTSTC

1. Introducción (iv)

■ Impacto económico:

THE GLOBAL PRICE TAG OF CONSUMER CYBERCRIME
\$113 BN
ENOUGH TO HOST THE 2012 LONDON OLYMPICS NEARLY 10 TIMES OVER
OTHER 37%
FRAUD 34%
RUMUS 24%
VIRUS/MALWARE 2%
USD \$298
AVERAGE COST PER VICTIM
REPRESENTS A 10 PERCENT INCREASE OVER 2012
Fuente: McAfee, 2014

THE GLOBAL PRICE TAG OF CONSUMER CYBERCRIME

Country	Cost (BN)
USA	38
MEXICO	13
EUROPE	13
INDIA	4
CHINA	37
SOUTH AFRICA	0.3
AUSTRALIA	1
RUSSIA	1
JAPAN	1

6

Internet Móvil - MIT
Tema 5: Seguridad móvil
© PGIT - DTSTC - UGR - 2017

DTSTC

Índice

1. Introducción
2. Fundamentos de seguridad
3. Arquitectura AAA
4. Gestión de la seguridad

Internet Móvil - MII
Tema 5: Seguridad móvil
© PGIT - DTSTC - UGR - 2017

2. Fundamentos de seguridad (i)

- **Seguridad:**
Protección de activos frente a amenazas, entendidas éstas como la capacidad potencial de mal uso de los activos protegidos
- **Activo:**
Elemento que forma parte de un sistema (hard/soft/persona)
- **Vulnerabilidad:**
Debilidad inherente al diseño, configuración o implementación de un sistema
- **Ataque:**
Instanciación de una amenaza

- "Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and General Model". Versión 3.1, Revisión 1, 2006.
- S. Furnell, S. Katsikas, J. López, A. Patel (editors). "Securing Information and Communications Systems". Artech House, 2008.

The diagram illustrates four types of attacks on a network flow:

- Interruption:** A node (R) removes a packet from the flow.
- Intercepción (Interception):** A node (A) receives a packet before its intended recipient (R).
- Modificación (Modification):** A node (A) changes a packet before it reaches its intended recipient (R).
- Fabricación (Fabrication):** A node (A) creates a packet and sends it to the intended recipient (R).

Below the diagram, boxes categorize these attacks:

- Modificación, Interrupción, Fabricación, Intercepción
- Activos (Actives), Pasivos (Passives)

Page number: 9

The diagram lists two main categories of attacks:

- Motivación atacantes: MEECES**
- Ejemplos de amenazas/riesgos:**

- Medioambientales
- Ingeniería social
- Intrusiones
- Escaneo de puertos
- Denegación de servicio (DoS)
- Spoofing*
- Hijacking*
- Botnets*
- Virus, troyanos, *spamming*, *phishing*, *rootkits*, *spyware*, *keyloggers*, *backdoors*, ...

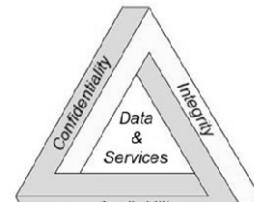
A cartoon illustration of a laptop screen showing a worm-like creature, labeled "Malware".

Page number: 10



2. Fundamentos de seguridad (iv)

- Servicios de seguridad:
 - Confidencialidad
 - Integridad
 - Disponibilidad
 - Autenticación
 - Responsabilidad:
 - Disuasión
 - No repudio
 - Recuperación



modelos CIA

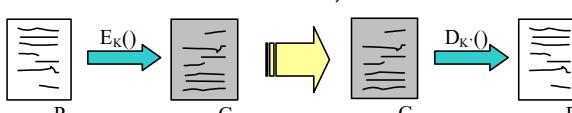
- Mecanismos de seguridad:
 - Cifrado
 - Firma digital
 - Autoridades certificación
 - Control de accesos

Internet Móvil - MII
Tema 5: Seguridad móvil
© PGIT - DTSTC - UGR - 2017
11



2. Fundamentos de seguridad (v) -Cifrado-

- Texto plano/claro, P → texto cifrado, C
 - Algoritmo cifrado/describrado: E(), D()
 - Clave de cifrado/descifrado: K, K'



Internet Móvil - MII
Tema 5: Seguridad móvil
© PGIT - DTSTC - UGR - 2017
12

* texto cifrado
* texto llano seleccionado
* texto plano conocido
* texto cifrado seleccionado



2. Fundamentos de seguridad (vi) -Cifrado-

- Tipos básicos de cifrado:
 - Cifrado de *bloque* vs. *flujo*
 - Sustitución
 - Transposición:

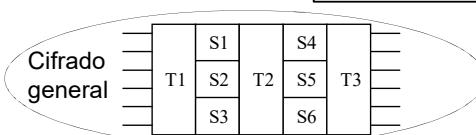
P: a b c d e f g h i j k l m n ñ o p q r s t u v w x y z }
 C: D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z A B C }

hola
 ↓
 KRÑD

P: transfiere un millón de euros a mi cuenta ⇒
 K: METANOL
 C: nunsnñrluiicitelucsndatfmemaaéoe ←

M	E	I	A	N	Q	L
4	2	7	1	5	6	3
t	r	a	n	s	f	i
e	r	e	u	n	m	i
l	l	ó	n	d	e	e
u	r	o	s	a	m	i
c	u	e	n	t	a	

Cifrado general

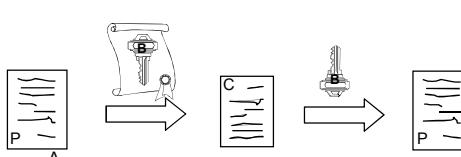


13



2. Fundamentos de seguridad (vii) -Cifrado-

- Cifrado simétrico: clave compartida emisor-receptor → DES, AES, RC4, ...
- Cifrado asimétrico: dos claves por usuario, pública (K_{pu}) y privada (K_{pr}) → RSA



14

2. Fundamentos de seguridad (viii)

-Autenticación de mensajes e integridad-

- MAC (“Message Authentication Code”):
 - $MAC_M = F(K_{AB}, M)$
 - $F()$ → DES, RC4, RSA, ...

15

2. Fundamentos de seguridad (ix)

-Autenticación de mensajes e integridad-

- Características funciones compendio:
 - De cálculo sencillo
 - Mensaje de salida de longitud fija
 - Dados P y P' distintos, sus compendios también lo son
 - Imposible obtener P a partir de su resumen: one-way

16

2. Fundamentos de seguridad (x)
-Autenticación del usuario-

- Clave compartida: reto-respuesta (p.e., RADIUS)

- Autenticación (y confidencialidad) con clave pública:

17

2. Fundamentos de seguridad (xi)
-Firma digital-

- Proporciona confidencialidad, autenticación e integridad:

18

2. Fundamentos de seguridad (xii)
-Gestión de claves-

- **Key Distribution Center : +no repudio**

```

graph LR
    A[A] -- "A, K_A(B, K_S)" --> KDC[KDC]
    KDC -- "K_B(A, K_S)" --> B[B]
    AS[AS] -- "A, B" --> A
    A -- "K_A(K_S, K_B(A, K_S))" --> AS
    AS -- "K_B(A, K_S), K_S(t)" --> B
    B -- "K_S(t+1)" --> A
  
```

□ Kerberos 5:
(RFC 4120)

19

2. Fundamentos de seguridad (xiii)
-Gestión de claves-

- Autenticación X.509:
 - Estándar ITU ampliamente usado (p.e., S/MIME, SSL, ...)

Optional

v2 v3

20

Índice

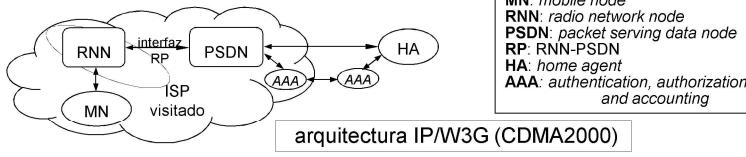


- 1. Introducción
- 2. Fundamentos de seguridad
- 3. Arquitectura AAA
- 4. Gestión de la seguridad

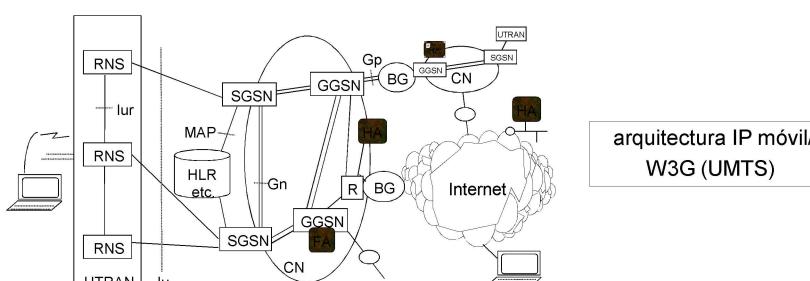
21

3. Arquitectura AAA

■ *Authentication, Authorization, Accounting:*

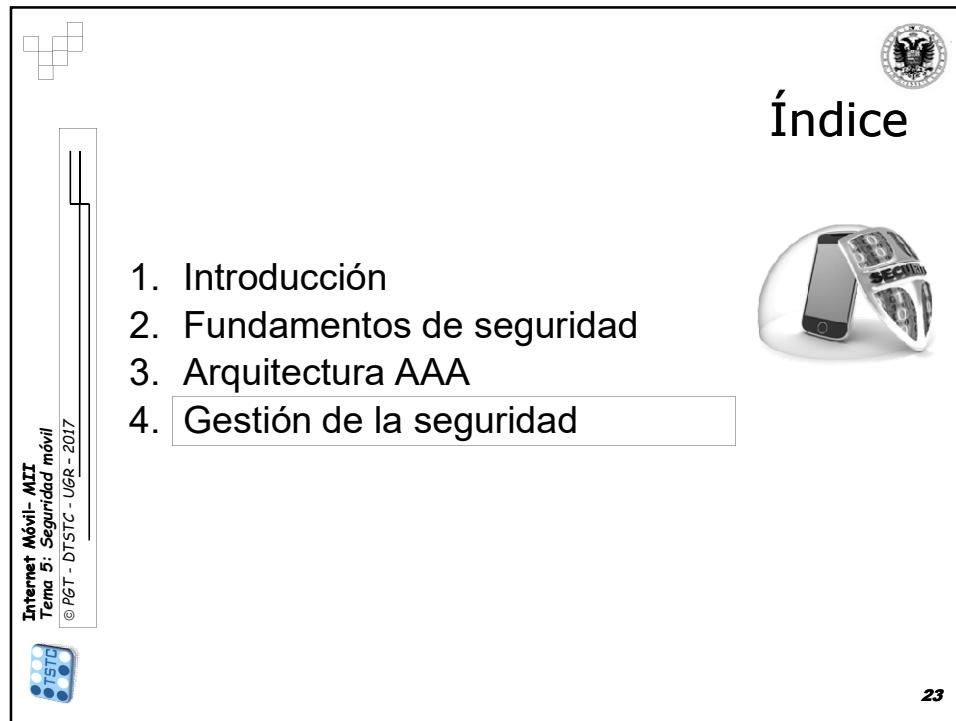


arquitectura IP/W3G (CDMA2000)



arquitectura IP móvil/W3G (UMTS)

22



The slide features a header with a small logo and text, followed by a large title 'Índice'. Below the title is a list of four items, with the fourth item 'Gestión de la seguridad' highlighted in a box. On the right side, there is a small image of a smartphone and a tablet. The footer contains the university seal, page number 23, and copyright information.

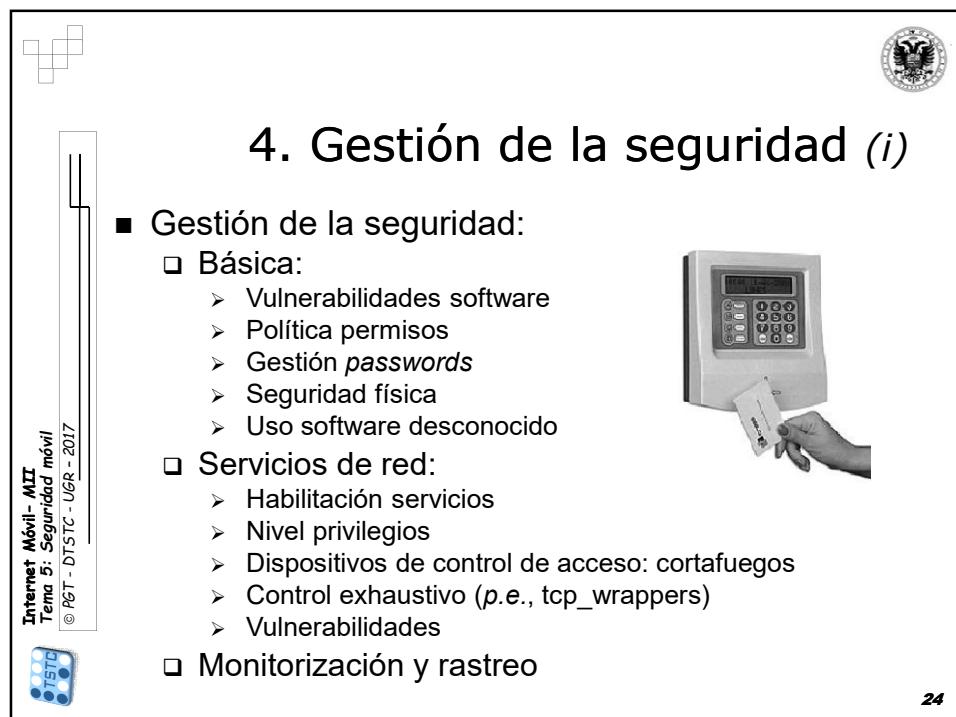
Índice

1. Introducción
2. Fundamentos de seguridad
3. Arquitectura AAA
4. Gestión de la seguridad

23

Internet Móvil - MII
Tema 5: Seguridad móvil
© PGIT - DTSTC - UGR - 2017

DTSTC



The slide features a header with a small logo and text, followed by a large title '4. Gestión de la seguridad (i)'. Below the title is a section titled '■ Gestión de la seguridad:' with three main points: 'Básica', 'Servicios de red', and 'Monitorización y rastreo'. To the right of the text, there is an image of a hand holding a card in front of a card reader. The footer contains the university seal, page number 24, and copyright information.

4. Gestión de la seguridad (i)

- Gestión de la seguridad:
 - Básica:
 - Vulnerabilidades software
 - Política permisos
 - Gestión *passwords*
 - Seguridad física
 - Uso software desconocido
 - Servicios de red:
 - Habilitación servicios
 - Nivel privilegios
 - Dispositivos de control de acceso: cortafuegos
 - Control exhaustivo (p.e., `tcp_wrappers`)
 - Vulnerabilidades
 - Monitorización y rastreo

24

Internet Móvil - MII
Tema 5: Seguridad móvil
© PGIT - DTSTC - UGR - 2017

DTSTC



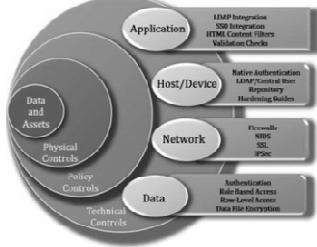
Internet Móvil - MII
Tema 5: Seguridad móvil
© PGIT - DTSTC - UGR - 2017





4. Gestión de la seguridad (ii) -Defensas-

- Seguridad en profundidad (*in-depth*):
 - Información *en tránsito* vs. información *estática*
 - Niveles de trabajo:
 - Redes, equipos y sistemas, aplicaciones/servicios, datos
- Líneas de defensa:
 1. Prevención
 2. Detección
 3. Respuesta




25



Internet Móvil - MII
Tema 5: Seguridad móvil
© PGIT - DTSTC - UGR - 2017





4. Gestión de la seguridad (iii) -Malware-

- Malware:
- Software malicioso incluido o insertado intencionadamente (y sin permiso) en un sistema para causar algún daño*
- Tipos:
 - Parásitos vs. independientes
 - Replicantes vs. no-replicantes

Name	Description
Virus	Malware that, when executed, tries to replicate itself into other executable code; when it succeeds the code is said to be infected. When the infected code is executed, the virus also executes.
Worm	A computer program that can run independently and can propagate a complete working version of itself onto other hosts on a network.
Logic bomb	A program inserted into software by an intruder. A logic bomb lies dormant until a predefined condition is met; the program then triggers an unauthorized act.
Trojan horse	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the Trojan horse program.
Backdoor (trapdoor)	Any mechanism that bypasses a normal security check; it may allow unauthorized access to functionality.
Mobile code	Software (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and execute with identical semantics.
Exploits	Code specific to a single vulnerability or set of vulnerabilities.
Downloader	Program that installs other items on a machine that is under attack. Usually, a downloader is sent in an e-mail.
Auto-rooter	Malicious hacker tools used to break into new machines remotely.
Ki (virus generator)	Set of tools for generating new viruses automatically.
Spammer programs	Used to send large volumes of unwanted e-mail.
Flooding	Used to attack networked computer systems with a large volume of traffic to carry out a denial-of-service (DoS) attack.
Keyloggers	Captures keystrokes on a compromised system.
Rootkit	Set of hacker tools used after attacker has broken into a computer system and gained root-level access.
Zombie, bot	Program activated on an infected machine that is activated to launch attacks on other machines.
Spyware	Software that collects information from a computer and transmits it to another system.
Adware	Advertising that is integrated into software. It can result in pop-up ads or redirection of a browser to a commercial site.

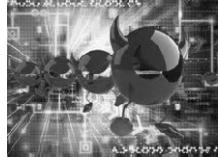
6





4. Gestión de la seguridad (iv) -Malware-

- Vías de infección del *malware*:
 - Dispositivos USB/CDs/DVDs infectados
 - Copias de programas (*¡con regalo!*)
 - Sitios web fraudulentos
 - Webs legítimas pero infectadas
 - Redes sociales
 - Redes P2P (*¡con regalo!*)
 - Adjuntos en correos no solicitados (*spam*)
 - Fallos de seguridad del propio S.O.



27

Internet Móvil - MIT
Tema 5: Seguridad móvil
© PGIT - DTSTC - UGR - 2017

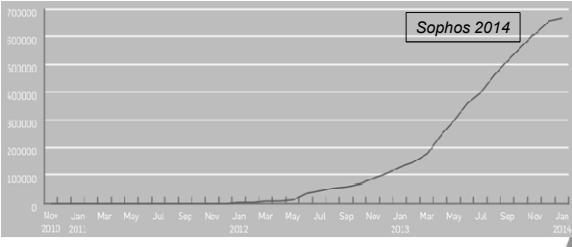




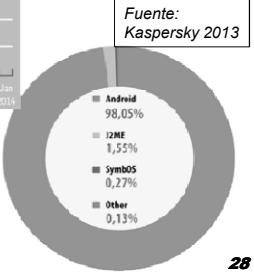


4. Gestión de la seguridad (v) -Malware-

- Evolución del *malware* para móviles:


Sophos 2014

- Afectación sistemas:


Fuente: Kaspersky 2013

Sistema Operativo	Porcentaje
Android	98,05%
iOS	1,55%
SymbOS	0,27%
Other	0,13%

28

Internet Móvil - MIT
Tema 5: Seguridad móvil
© PGIT - DTSTC - UGR - 2017



4. Gestión de la seguridad (vi)
-Malware-

□ Impacto:

Fuente:
Kaspersky 2013

Internet Móvil - MII
Tema 5: Seguridad móvil
© PGIT - DTSTC - UGR - 2017

29

4. Gestión de la seguridad (vii)
-Malware-

□ Vectores de infección:

Formas de afectación

- Descargas web
- App stores alternativas
- SMS
- Correo electrónico
- Vulnerabilidades sistemas:

debilidades de diseño y/o implementación

Internet Móvil - MII
Tema 5: Seguridad móvil
© PGIT - DTSTC - UGR - 2017

30

4. Gestión de la seguridad (viii)
-Malware-

□ Software malicioso en móviles:

Malware Type	Percentage
Trojan-SMS	36%
Backdoor	26%
Trojan	16%
Trojan-Downloader	7%
Other	15%

Fuente:
Kaspersky 2013

31

Internet Móvil - MII
Tema 5: Seguridad móvil
© PGIT - DTSTC - UGR - 2017

DTSTC

4. Gestión de la seguridad (ix)
-Malware-

□ 10 familias más populares en 2013:

Name*	% of all attacks
DangerousObject Multi Generic	40.42%
Trojan-SMS.AndroidOS.OpFake.bo	21.77%
AdWare.AndroidOS.Ganlet.a	12.40%
Trojan-SMS AndroidOS.FakeInst.a	10.37%
RiskTool.AndroidOS.SMSreg.cw	8.80%
Trojan-SMS.AndroidOS.Agent.u	8.03%
Trojan-SMS.AndroidOS.OpFake.a	5.49%
Trojan.AndroidOS.Plangton.a	5.37%
Trojan.AndroidOS.MTK.a	4.25%
AdWare.AndroidOS.Hamob.a	3.39%

Fuente:
Kaspersky 2013

32

Internet Móvil - MII
Tema 5: Seguridad móvil
© PGIT - DTSTC - UGR - 2017

DTSTC

4. Gestión de la seguridad (x)
-Malware-

□ Ataques Android:

○ Andr/BBridge-A	9%	○ Andr/Adop-A	2%	○ Andr/SmsSend-BF	2%
○ Andr/Fakeins-V	6%	○ Andr/Bixer-D	2%	○ Andr/MTK-B	2%
○ Andr/Generic-S	5%	○ Andr/SmsSend-BY	2%	● Other	65%
○ Andr/Qdplugin-A	3%	○ Andr/DroidRt-A	2%		

Fuente:
Sophos 2014

33

4. Gestión de la seguridad (xi)
-Malware-

□ Ejemplos:

- Falso media player e instalación del usuario desde una web infectada.
- Rootkit en forma de módulo kernel descargable que puede abrir un shell para el atacante ante la recepción de una llamada entrante desde un cierto número
 - ⇒ Acceso a SMS, GPS, llamadas de voz, etc.

34

**4. Gestión de la seguridad (xii)
-Malware-**

❑ Troyanos bancarios:

Mes	Instancias
2013.01	~50
2013.02	~70
2013.03	~100
2013.04	~150
2013.05	~200
2013.06	~250
2013.07	~300
2013.08	~400
2013.09	~650
2013.10	~900
2013.11	~1200
2013.12	~1350

Fuente:
Kaspersky 2013

❑ Svpeng ❑ Perkele ❑ Wroba

35

**4. Gestión de la seguridad (xiii)
-Malware-**

❑ Anatomía de un móvil *hackeado* y efectos:

Android malware instances seen by SophosLabs: 350,000

Smartphones lost every minute in the U.S.: 113

Average cost of a U.S. data breach in 2012: \$5.4 million

Price charged by the Android Defender ransomware*: \$99.99

*Source: SophosLabs
**Source: 2013 Cost of Data Breach Study, Ponemon Institute
**Source: What's the Worst U.S. City for Smartphone Theft?, Mashable

36





4. Gestión de la seguridad (xiv)

-Malware-

Consejos para prevenir *malware*:

1. Informar usuarios sobre riesgos
2. Seguridad en accesos (p.ej., criptografía)
3. Políticas BYOD ("bring your own device")
4. Evitar *jailbreak*
5. Actualizar equipos y sistemas
6. Cifrado de dispositivos
7. Políticas de seguridad móvil
8. Instalar *apps* de fuentes confiables
9. Compartición en nube
10. Software *anti-malware* ...



37

Internet Móvil - MIT
Tema 5: Seguridad móvil
© PGIT - DTSTC - UGR - 2017







4. Gestión de la seguridad (xv)

-Malware-

Software seguridad móvil:

- *Network Log*: monitoriza las conexiones de red de las aplicaciones instaladas
- *OS Monitor*: controla los procesos y las conexiones de cada aplicación
- *SmartDroid*: envío de notificaciones ante detección de ciertos eventos, definidos por el usuario (*firmas*)
- *CONAN mobile*: indica nivel de seguridad, monitoriza las aplicaciones y los permisos y mantiene listas de IP y números llamados



38

Internet Móvil - MIT
Tema 5: Seguridad móvil
© PGIT - DTSTC - UGR - 2017







4. Gestión de la seguridad (xvi)

-Malware-

Software seguridad móvil (cont.):

- *ComDroid, Woodpecker*: permisos entre aplicaciones
- *DroidMOSS*: similitud *fuzzy* entre apps para detectar cambios
- *RiskRanker*: comportamientos peligrosos pre-definidos
- *DREBIN*: aplicaciones maliciosas/benignas mediante SVM
- *Andromaly*: detección de anomalías *machine-learning* (ML)
- *MADAM*: uso de características *kernel/user-based* y ML
- *Crowdroid*: detección de troyanos basada en llamadas al sistema
- *DroidAPIMiner*: uso de características *API-based* y KNN
- *TaintDroid*: monitorización de datos privados sensibles

Retos: *lightweight* → detección “colaborativa”



39

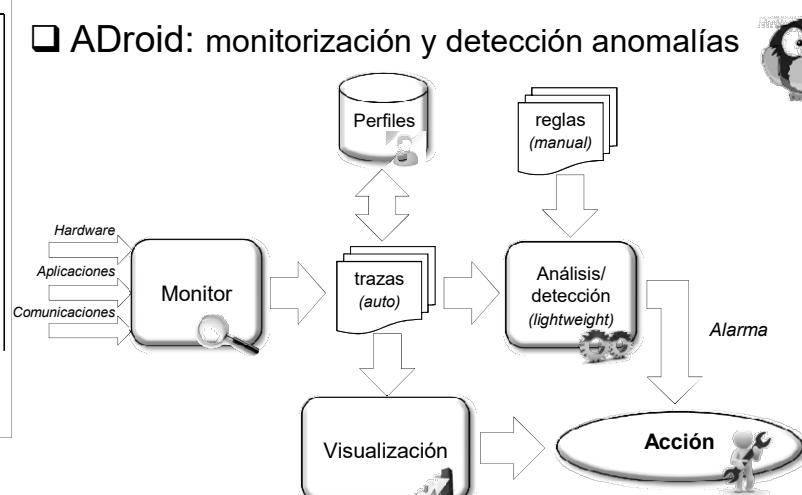




4. Gestión de la seguridad (xvii)

-Malware-

ADroid: monitorización y detección anomalías



40