

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



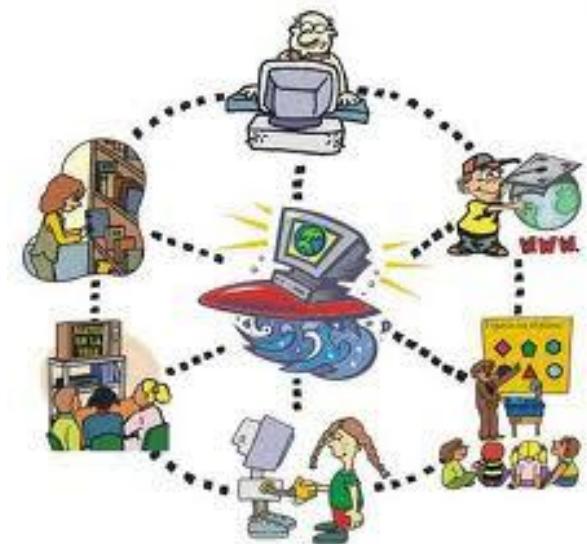
Índice

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



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



1. Introducción (ii)

■ Complejidad sistemas actuales:



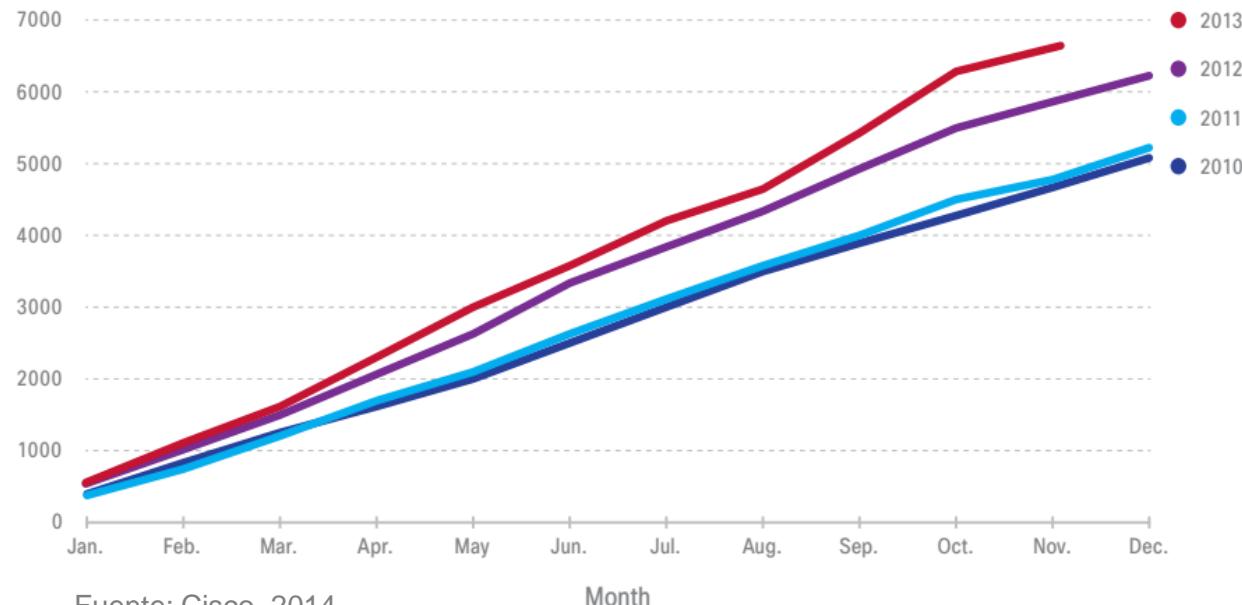


1. Introducción (iii)

■ Evolución vulnerabilidades:



Cumulative Annual Alert Totals, 2010-2013



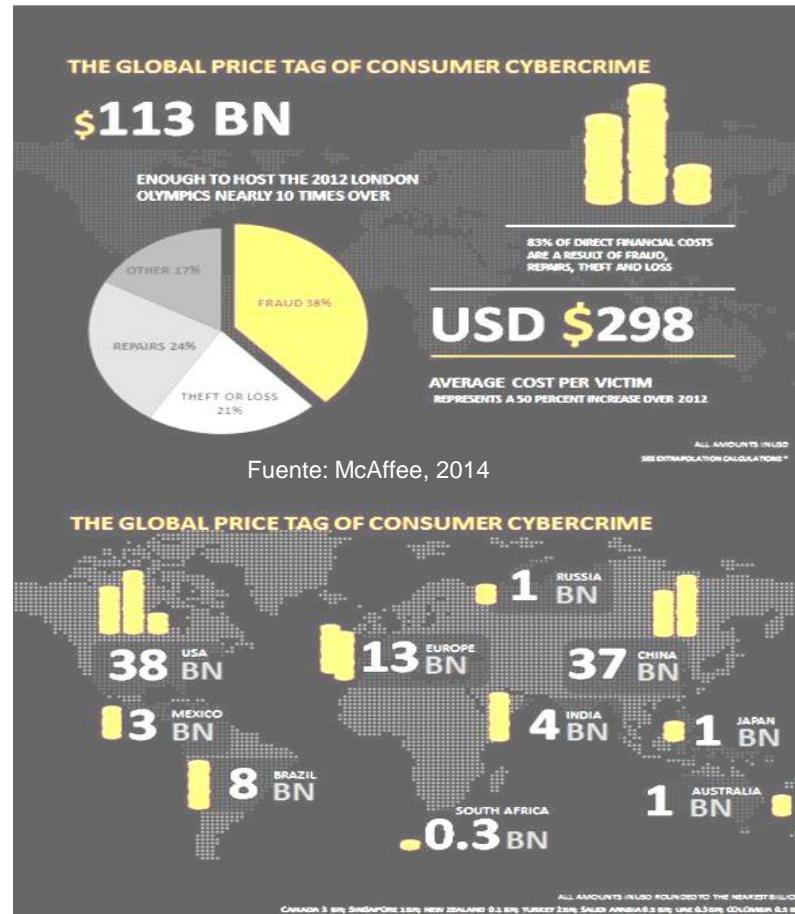
Fuente: Cisco, 2014

Month



1. Introducción (iv)

■ Impacto económico:





Índice

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





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:

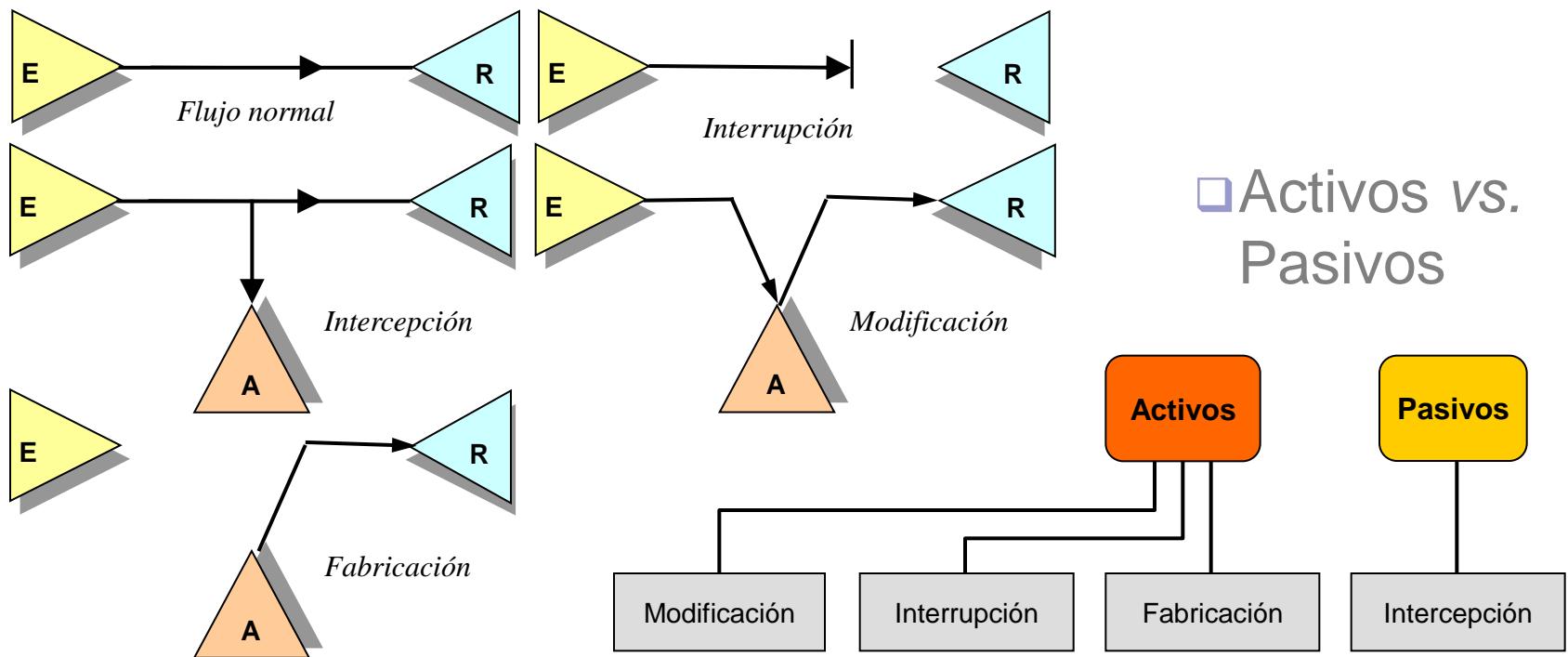
Instanciación de una amenaza

-
- "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.



2. Fundamentos de seguridad (ii)

- Tipos de ataques:
 - Interrupción vs. Intercepción vs. Modificación vs. Fabricación



2. Fundamentos de seguridad (iii)

- 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*, ...



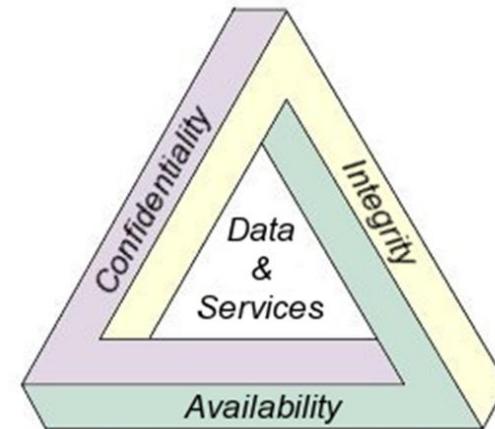


2. Fundamentos de seguridad (iv)

■ Servicios de seguridad:

- Confidencialidad
- Integridad
- Disponibilidad
- Autenticación
- Responsabilidad:
 - Disuasión
 - No repudio
 - Recuperación

} *modelo CIA*



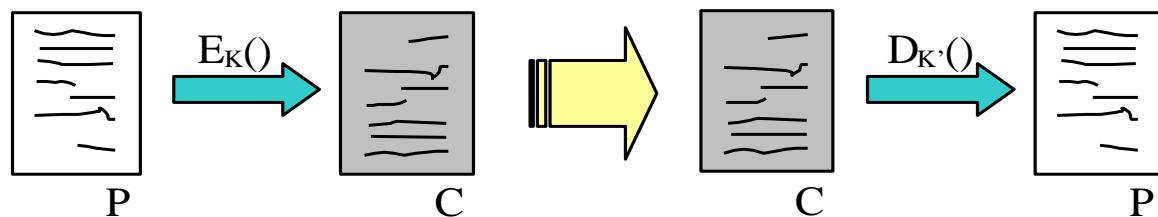
■ Mecanismos de seguridad:

- Cifrado
- Firma digital
- Autoridades certificación
- Control de accesos

2. Fundamentos de seguridad (v)

-Cifrado-

- Texto plano/claro, $P \rightarrow$ texto cifrado, C
 - Algoritmo cifrado/descrifrado: $E()$, $D()$
 - Clave de cifrado/descifrado: K , K'



- Requisitos:
 - $E()$ y $D()$ de bajo coste computacional y sencillas
 - $E(P) \neq E(P')$ y $D(C) \neq D(C')$, $\forall P \neq P'$ y $C \neq C'$
 - Robustez ante criptoanálisis:
 - * 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

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 }

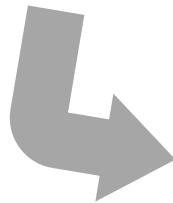
hola
 ↓
 KRÑD

- Transposición:

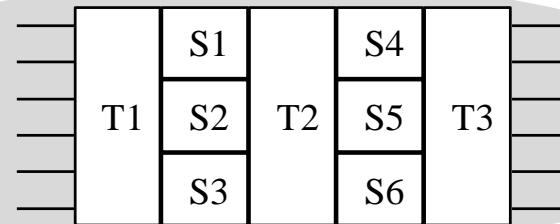
P: transfiere un millón de euros a mi cuenta ⇒
K: METANOL

C: nunsnrrlruuiieitelucsndatfmemaaeóoe

M	E	T	A	N	O	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	



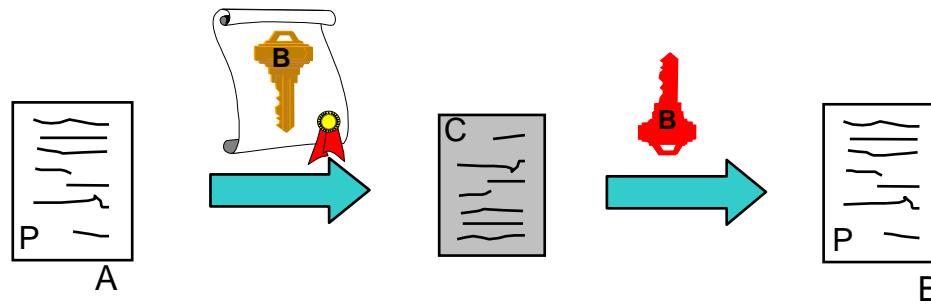
Cifrado
general



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

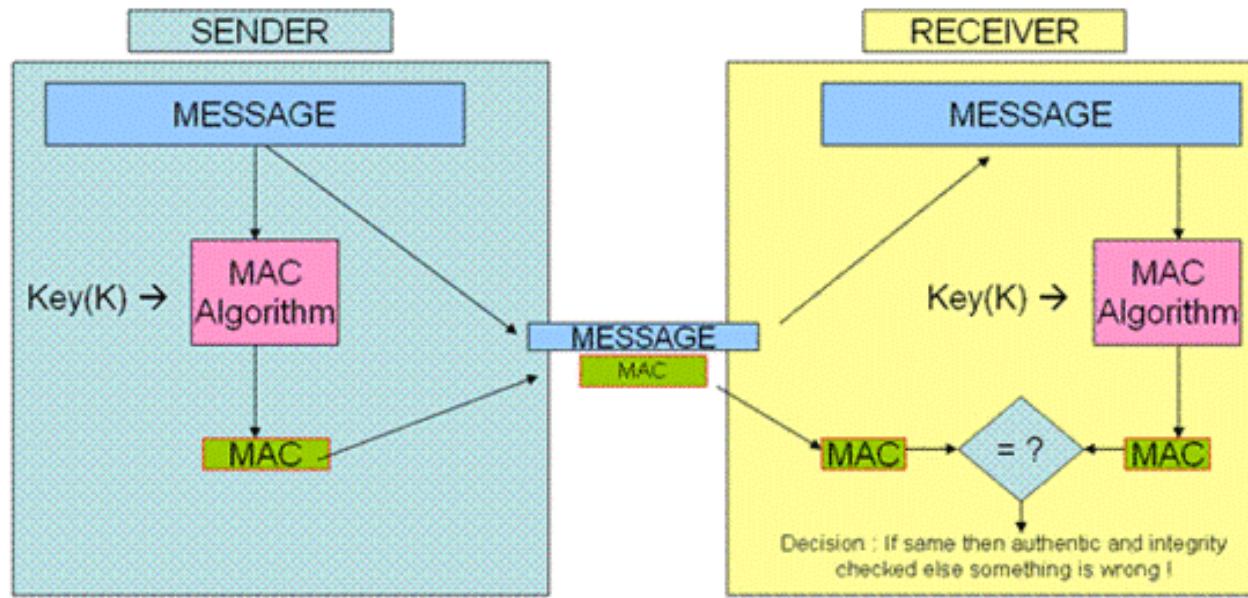


2. Fundamentos de seguridad (viii)

-Autenticación de mensajes e integridad-

■ MAC (“Message Authentication Code”):

- $MAC_M = F(K_{AB}, M)$
- $F()$ → DES, RC4, RSA, ...



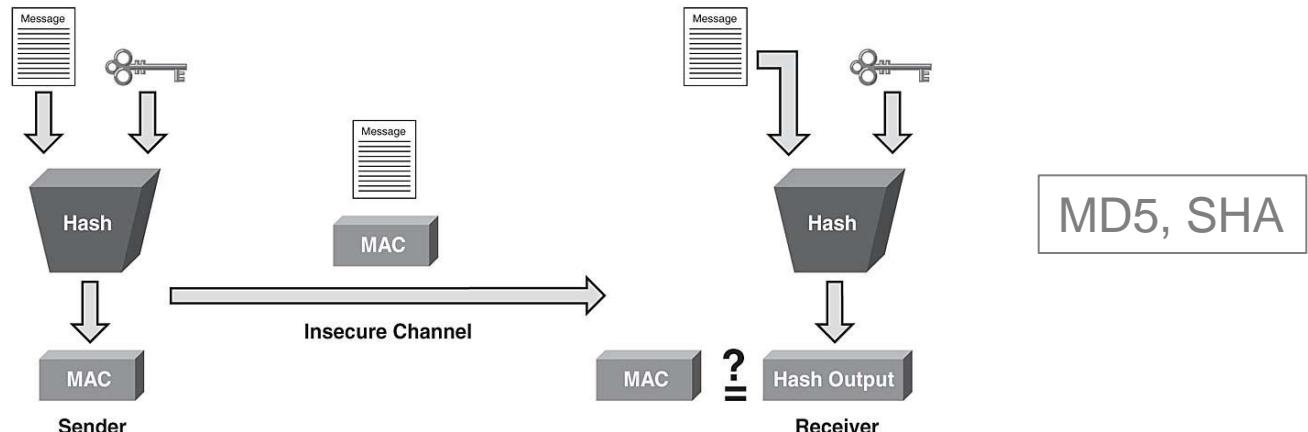


2. Fundamentos de seguridad (ix)

-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

$$\begin{aligned} & \frac{(y+8x^2+27x^3)y_1 + x_2(y_2y_3 + c_1(x)y_3)}{y^2} \\ &= \left(\frac{x(x-2)}{2} \right) 1 + (x(x-2))0 + \left(\frac{x(x-1)}{2} \right) \\ &= \left(\frac{x-1}{2}(x-2) \right) 1 + (x(x-1))0 \neq \frac{x+1}{2} \\ &\frac{y^2(y+6x^2+4x^3)(x+9)}{x(x+6)^2} \neq \frac{y^2(y+6x^2+4x^3)(x+9)}{x(x+6)^2} \end{aligned}$$



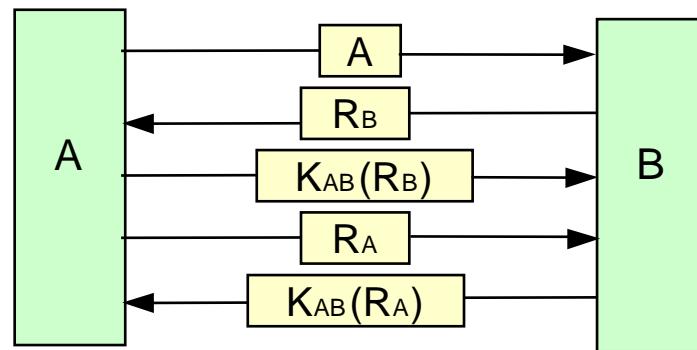
MD5, SHA



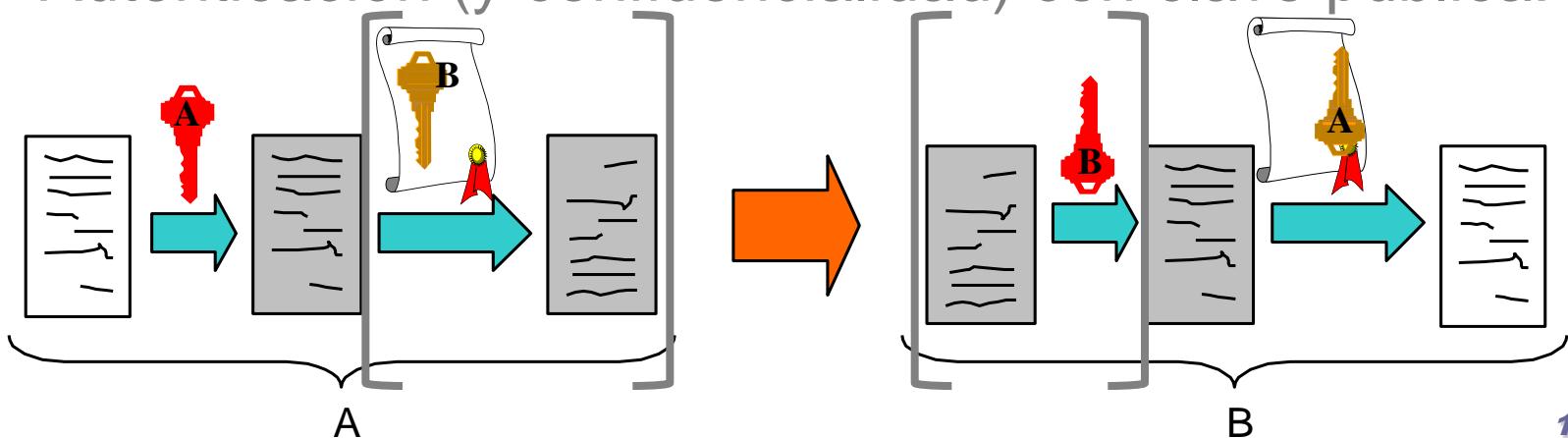
2. Fundamentos de seguridad (x)

-Autenticación del usuario-

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



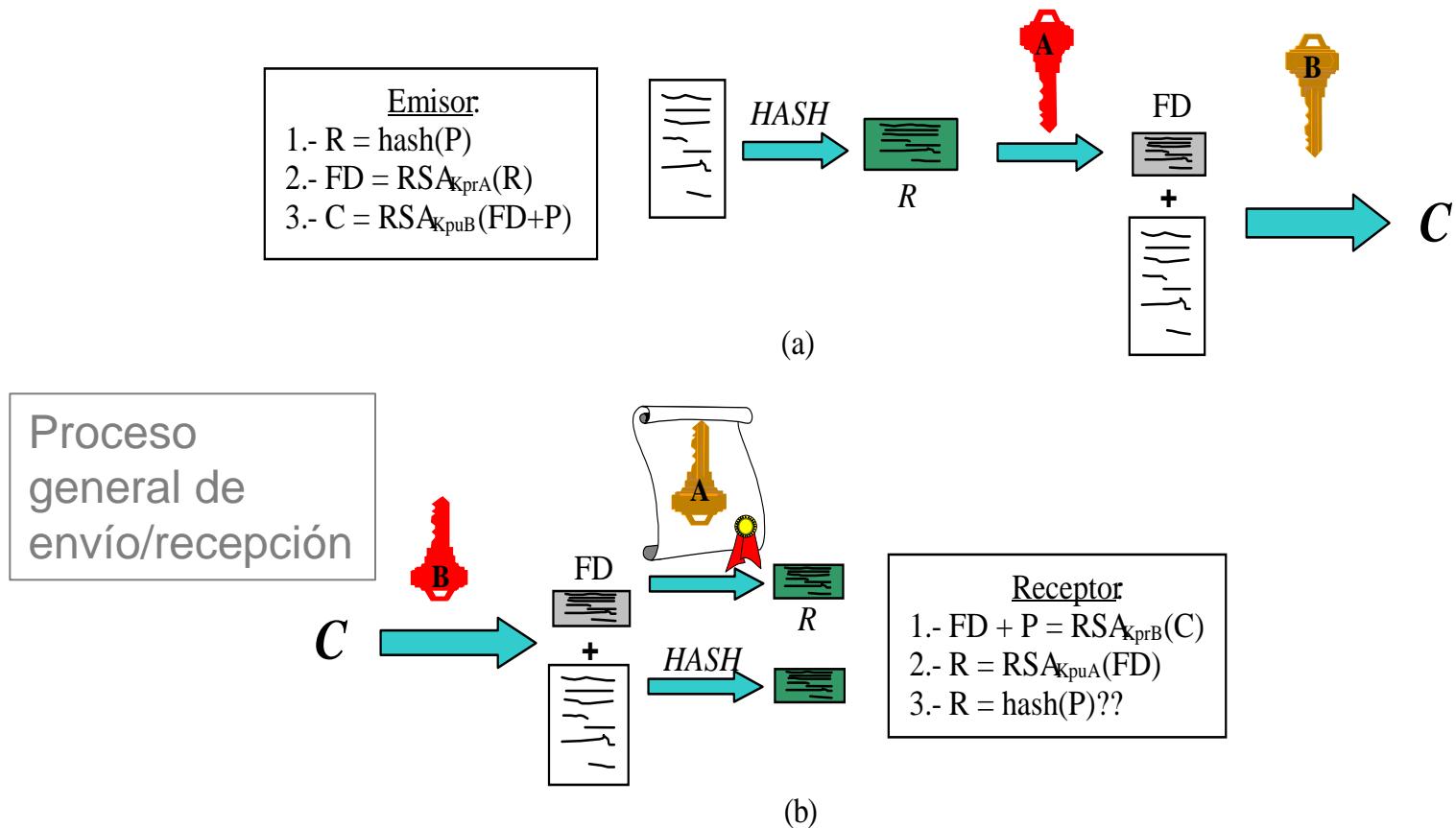
- Autenticación (y confidencialidad) con clave pública:



2. Fundamentos de seguridad (xi)

-Firma digital-

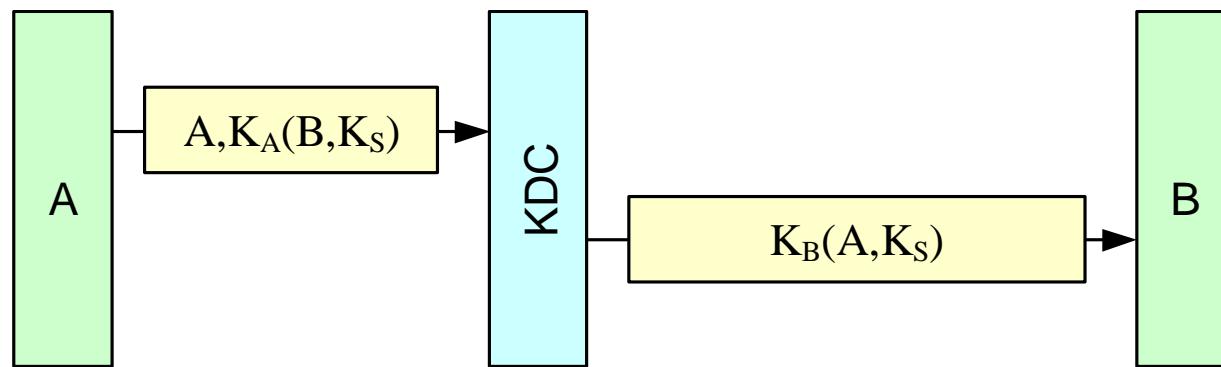
- Proporciona confidencialidad, autenticación e integridad:



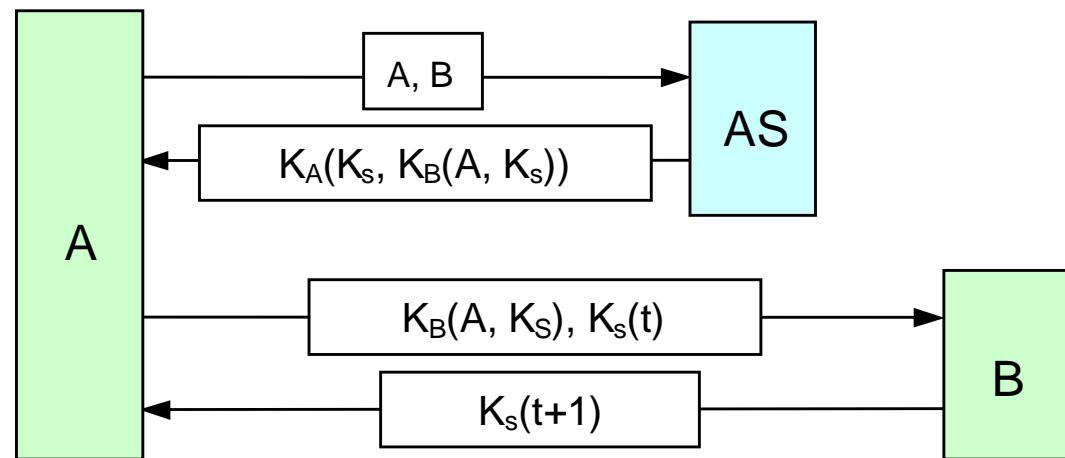
2. Fundamentos de seguridad (xii)

-Gestión de claves-

- Key Distribution Center : +no repudio



- Kerberos 5:
(RFC 4120)



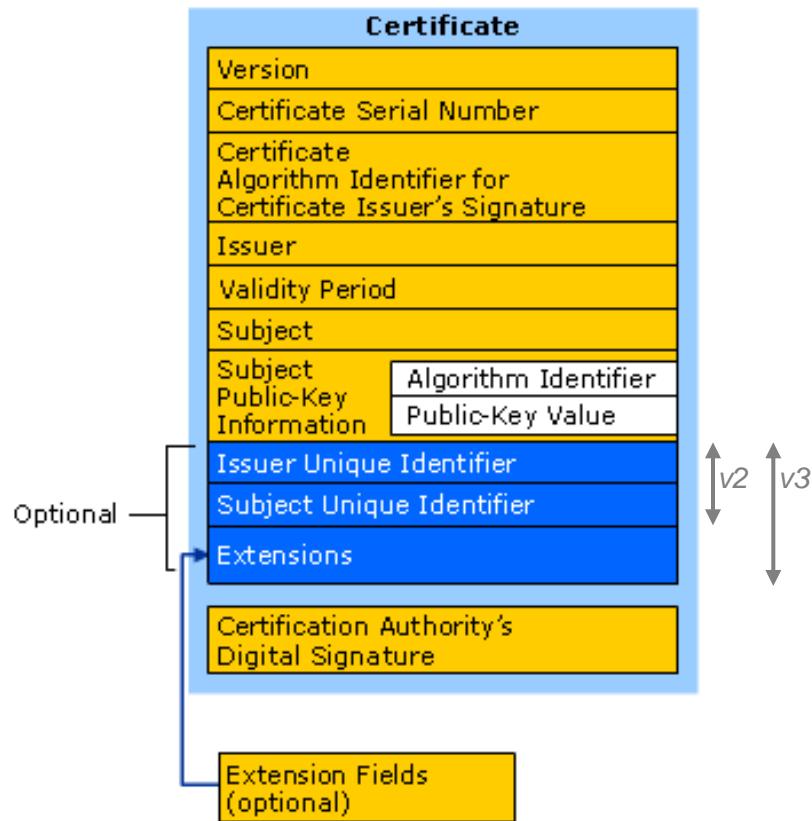


2. Fundamentos de seguridad (xiii)

-Gestión de claves-

■ Autenticación X.509:

- Estándar ITU ampliamente usado (p.e., S/MIME, SSL, ...)





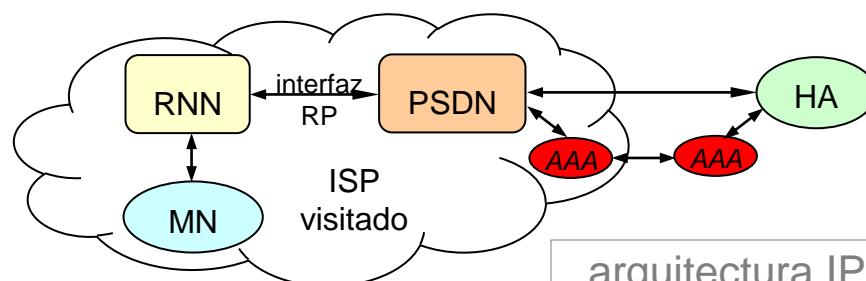
Índice

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



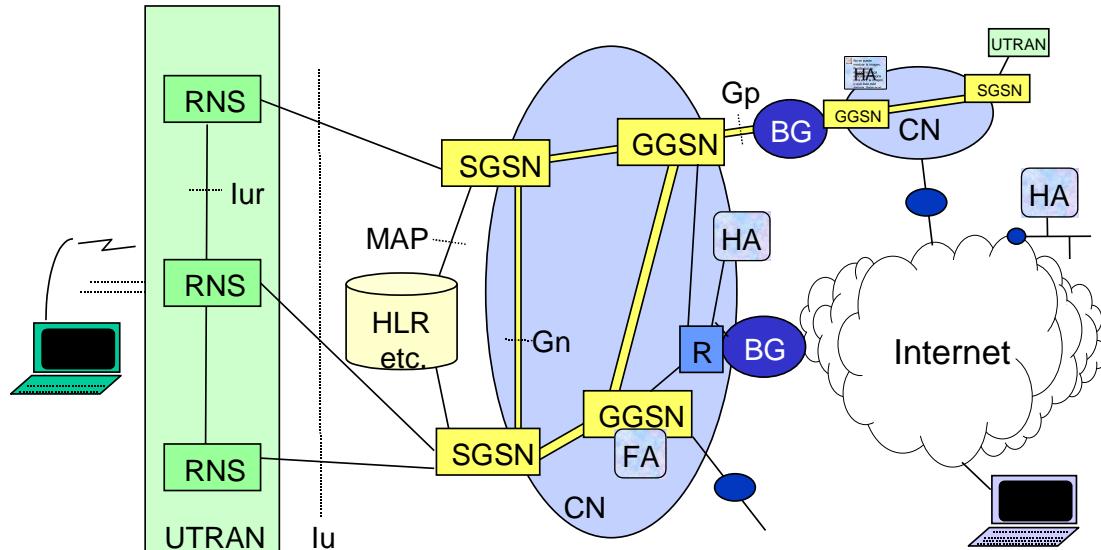
3. Arquitectura AAA

■ Authentication, Authorization, Accounting:



MN: mobile node
RNN: radio network node
PSDN: packet serving data node
RP: RNN-PSDN
HA: home agent
AAA: authentication, authorization and accounting

arquitectura IP/W3G (CDMA2000)



arquitectura IP móvil/
W3G (UMTS)



Índice

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





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

4. Gestión de la seguridad (ii)

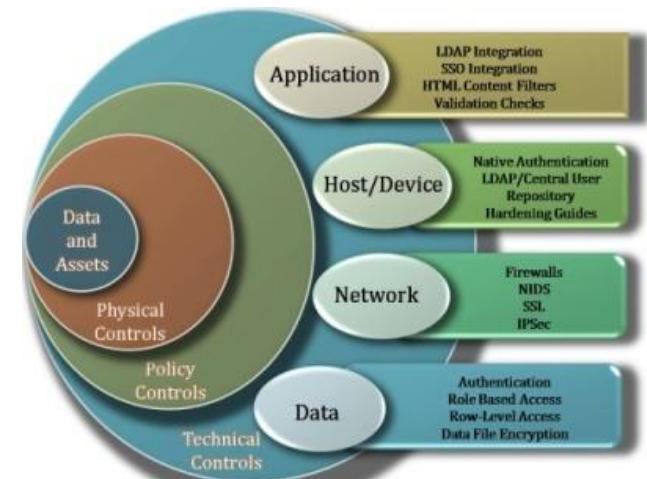
-Defensas-

■ 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





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.
Downloaders	Program that installs other items on a machine that is under attack. Usually, a downloader is sent in an e-mail.
Auto-router	Malicious hacker tools used to break into new machines remotely.
Kit (virus generator)	Set of tools for generating new viruses automatically.
Spammer programs	Used to send large volumes of unwanted e-mail.
Flooders	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.

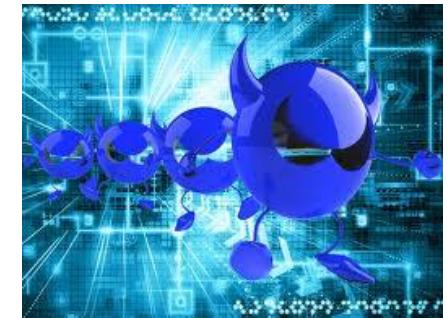


4. Gestión de la seguridad (iv)

-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.

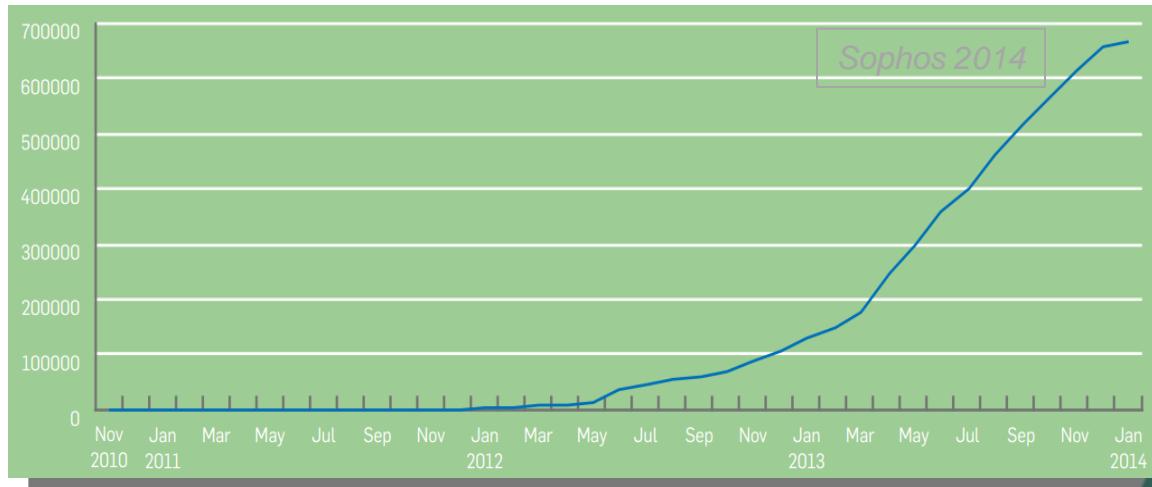




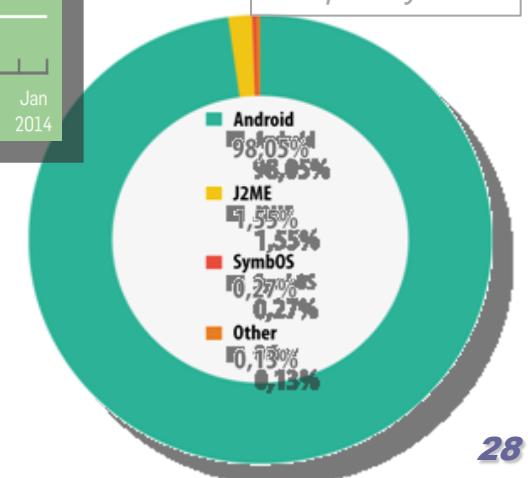
4. Gestión de la seguridad (v)

-Malware-

- Evolución del *malware* para móviles:



Fuente:
Kaspersky 2013

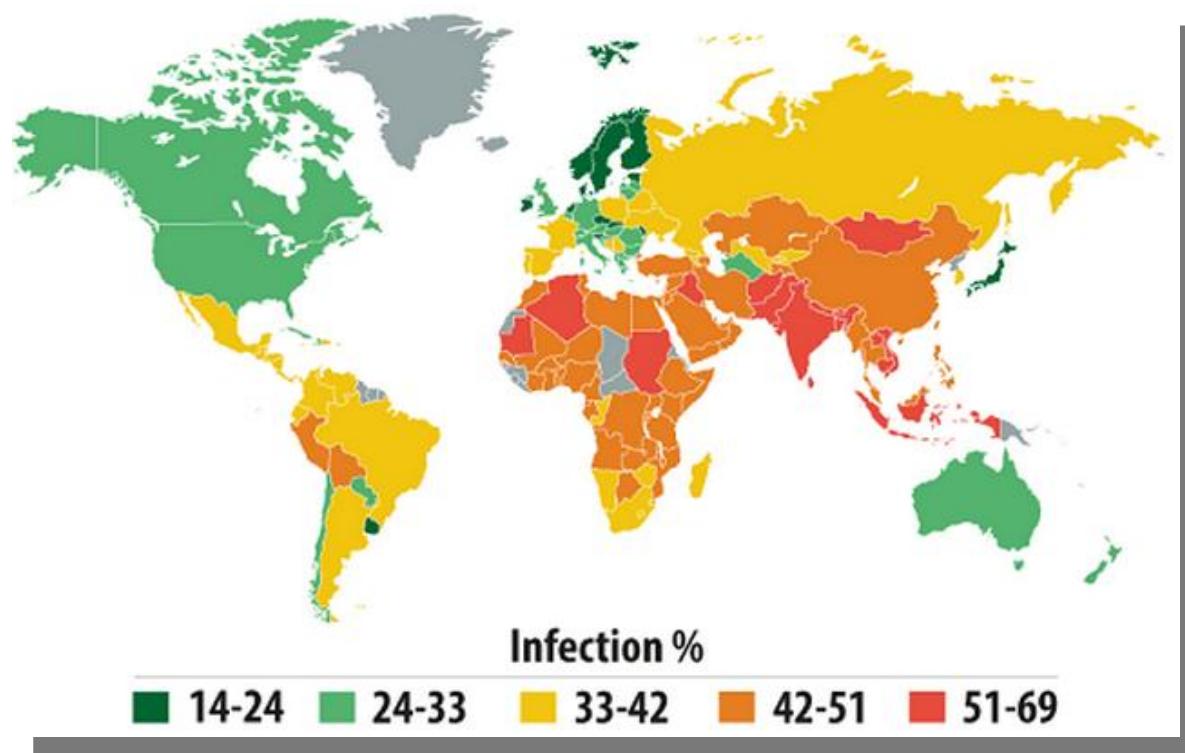


- Afectación sistemas:

4. Gestión de la seguridad (vi)

-Malware-

Impacto:



4. Gestión de la seguridad (vii)

-Malware-

Vectores de infección:

Formas de afectación

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

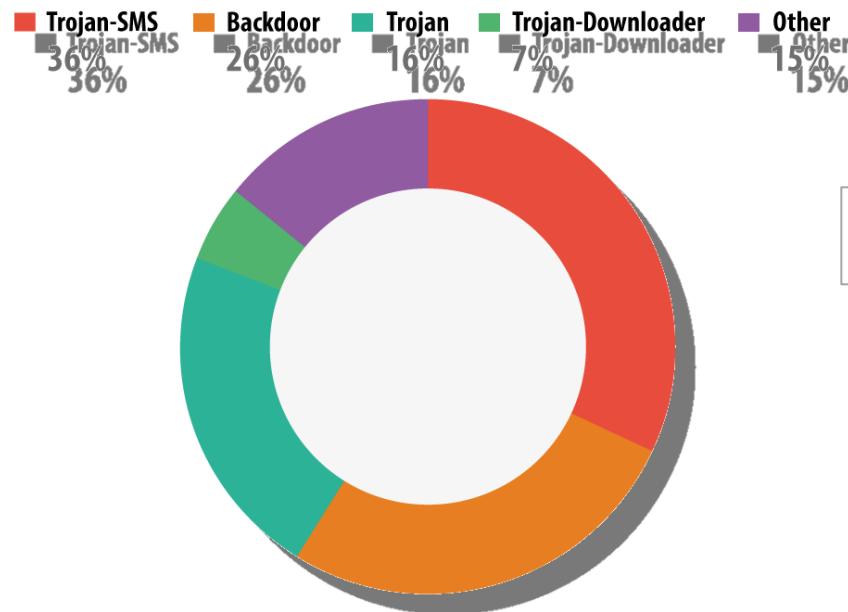
debilidades de diseño y/o implementación



4. Gestión de la seguridad (viii)

-Malware-

□ Software malicioso en móviles:



Fuente:
Kaspersky 2013



4. Gestión de la seguridad (ix)

-Malware-

- 10 familias más populares en 2013:

	Name*	% of all attacks
1	DangerousObject.Multi.Generic	40.42%
2	Trojan-SMS.AndroidOS.OpFake.bo	21.77%
3	AdWare.AndroidOS.Ganlet.a	12.40%
4	Trojan-SMS.AndroidOS.FakeInst.a	10.37%
5	RiskTool.AndroidOS.SMSreg.cw	8.80%
6	Trojan-SMS.AndroidOS.Agent.u	8.03%
7	Trojan-SMS.AndroidOS.OpFake.a	5.49%
8	Trojan.AndroidOS.Plangton.a	5.37%
9	Trojan.AndroidOS.MTK.a	4.25%
10	AdWare.AndroidOS.Hamob.a	3.39%

Fuente:
Kaspersky 2013

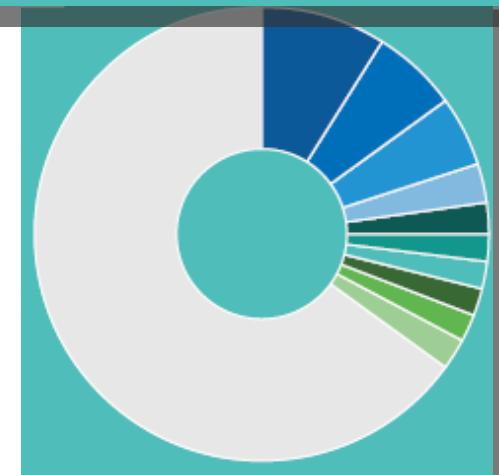


4. Gestión de la seguridad (x)

-Malware-

□ Ataques Android:

○ Andr/BBridge-A	9%	○ Andr/Adop-A	2%	○ Andr/SmsSend-BE	2%
○ Andr/Fakeins-V	6%	○ Andr/Boxer-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					





4. Gestión de la seguridad (xi)

-Malware-

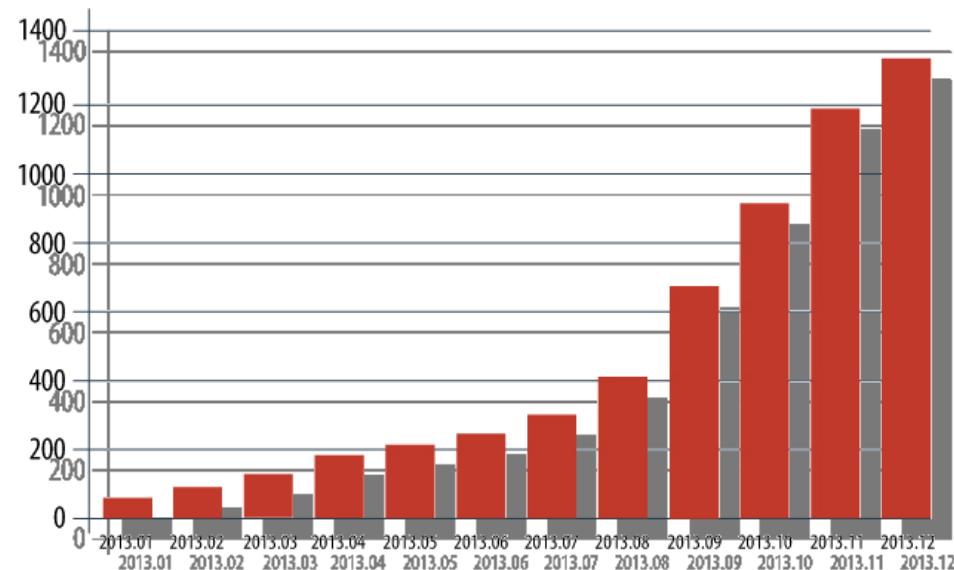
□ Ejemplos:

- Falseo *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.

4. Gestión de la seguridad (xii)

-Malware-

Troyanos bancarios:



Fuente:
Kaspersky 2013

Svpeng

Perkele

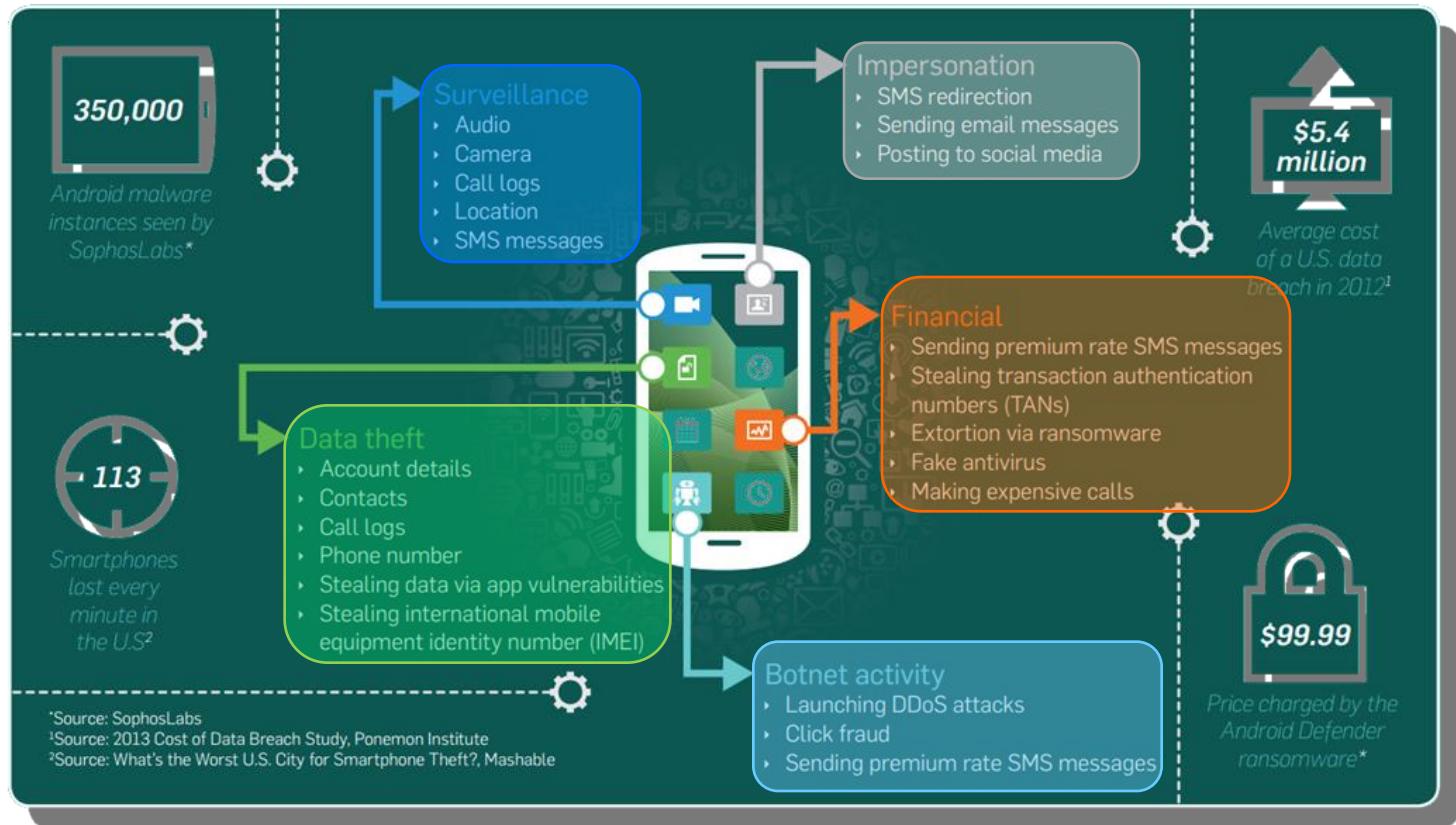
Wroba



4. Gestión de la seguridad (xiii)

-Malware-

□ Anatomía de un móvil *hackeado* y efectos:





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* ...





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





4. Gestión de la seguridad (xvi)

-Malware-

- Software seguridad móvil (*cont.*):
 - *ComDroid*, *Woodpeker*: 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”

4. Gestión de la seguridad (xvii)

-Malware-

- ADroid: monitorización y detección anomalías

