Bugs & Kisses

Spying on BlackBerry users for fun

Troopers Security Conference 2010

Social Engineering

The clever manipulation of the natural human tendency to trust.

"There's one born every minute."

There's always a chance you will get 0wned.

Friday, March 12, 2010


BlackBerry
space

Push Email

QWERTY Keyboard

Granular Security Controls

Transport Level Security

Device Encryption

Granular Controls

Allow or deny access to User Data

Allow or deny access to Application Interaction

Allow or deny access to Internet Connectivity

Transport Security

Traffic is encrypted up to RIM in Canada

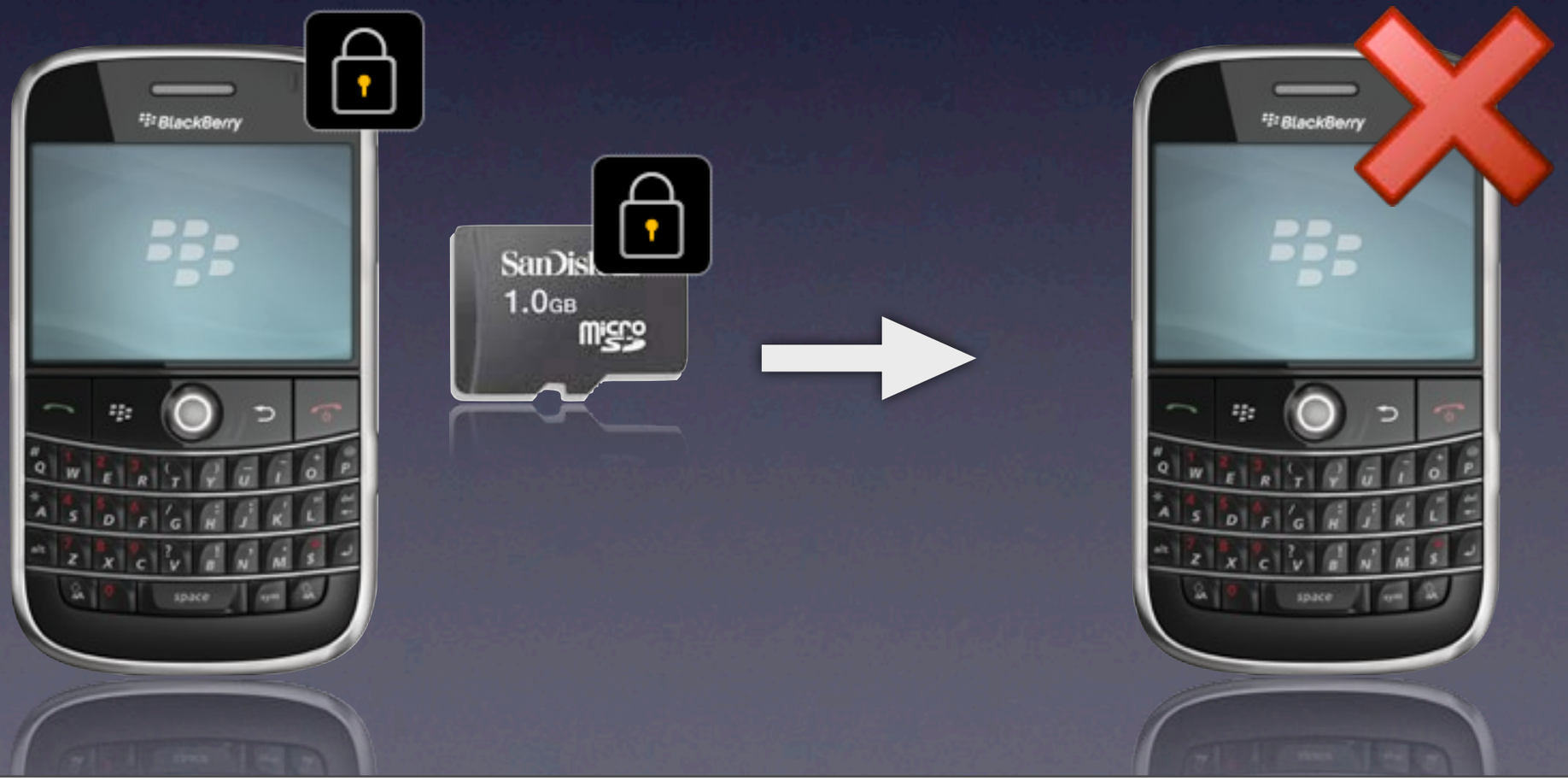
Cannot MITM

Even HTTP traffic goes over a tunnel

Device Encryption

Memory and micro-SD card cannot be read on another device

Stolen, encrypted devices are still safe



Granular Security Controls

Transport Level Security

Device Encryption

2

39

Vulnerabilities on SecurityFocus - Sep ’09

Personal Information?

Personal (read 'naughty') pictures

Private text messages

Emails with passwords, contracts, personal info

Phone Call Logs; who have you been calling?

A Few Problems

We can't hack it - no useful vulnerabilities

We can't MITM - everything is encrypted

We could steal it...

APIs

Text Messages

Package: **javax.wireless.messaging**

Interface: **MessageListener**

Methods: **setMessageListener()**

- Receive and Send SMS messages without owner's knowledge


BlackBerry


Listener

Demo

Bugs

Posts email to TROOPERS 10 - Wall of Geese

Download:

http://www.zensay.com/Bugs.jad

Wall of Geese:

http://www.zensay.com/geese.php

APIs

Email Messages

Package: **net.rim.blackberry.api.mail.event**

Interface: **FolderListener**

Methods: **messagesAdded()**

- Intercept and forward all emails on the BlackBerry handheld

- Send spoofed email from the device

APIs

Remote Listening

Package: **net.rim.blackberry.api.phone**

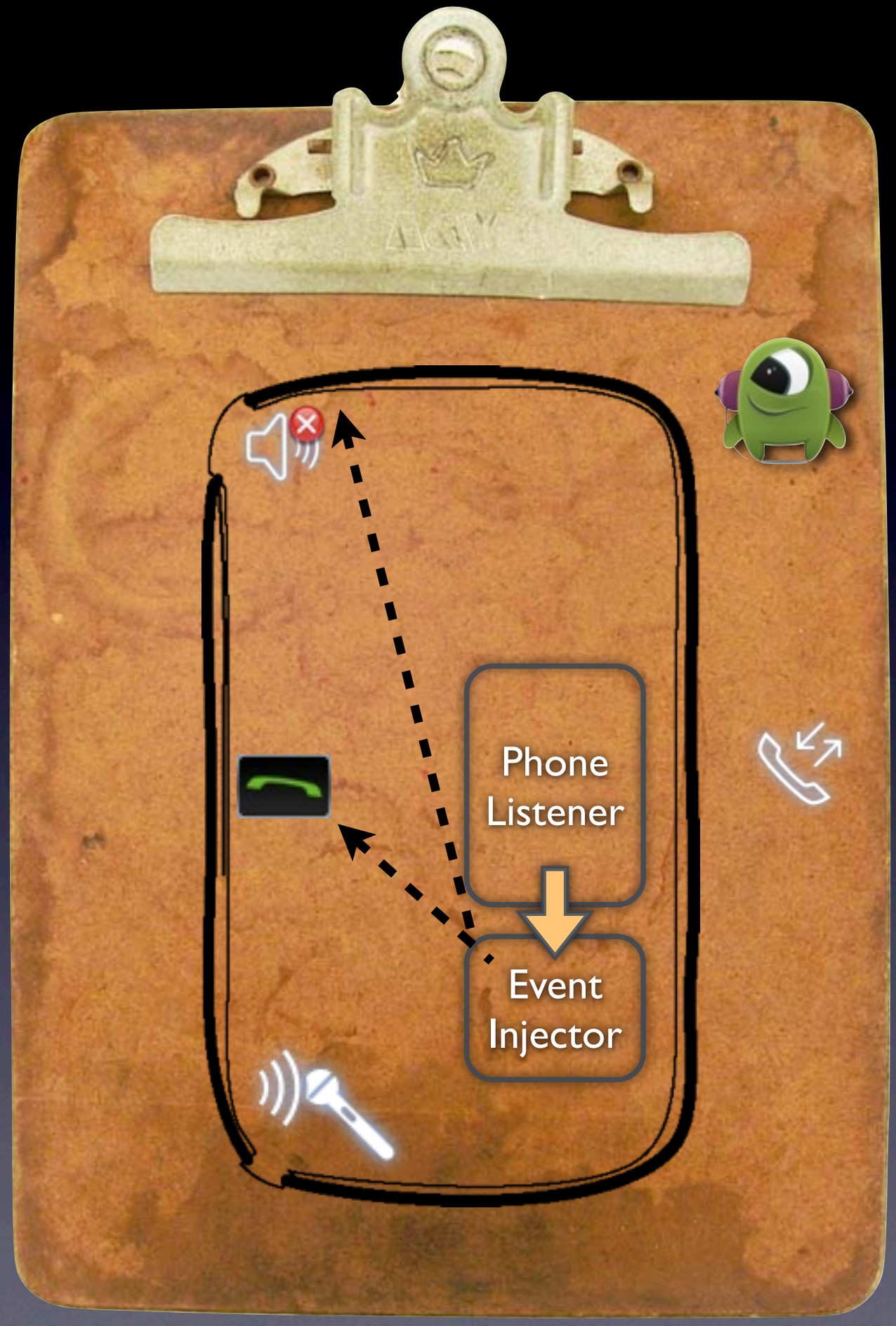
Interface: **PhoneListener**

Methods: **EventInjector.invokeEvent()**

- Silently intercept phone call, turn microphone on and listen in

- Portable bugging device


BlackBerry


Phone
Listener
Event
Injector

Demo

APIs

Remote Listening Part 2

Package: **javax.microedition.media**

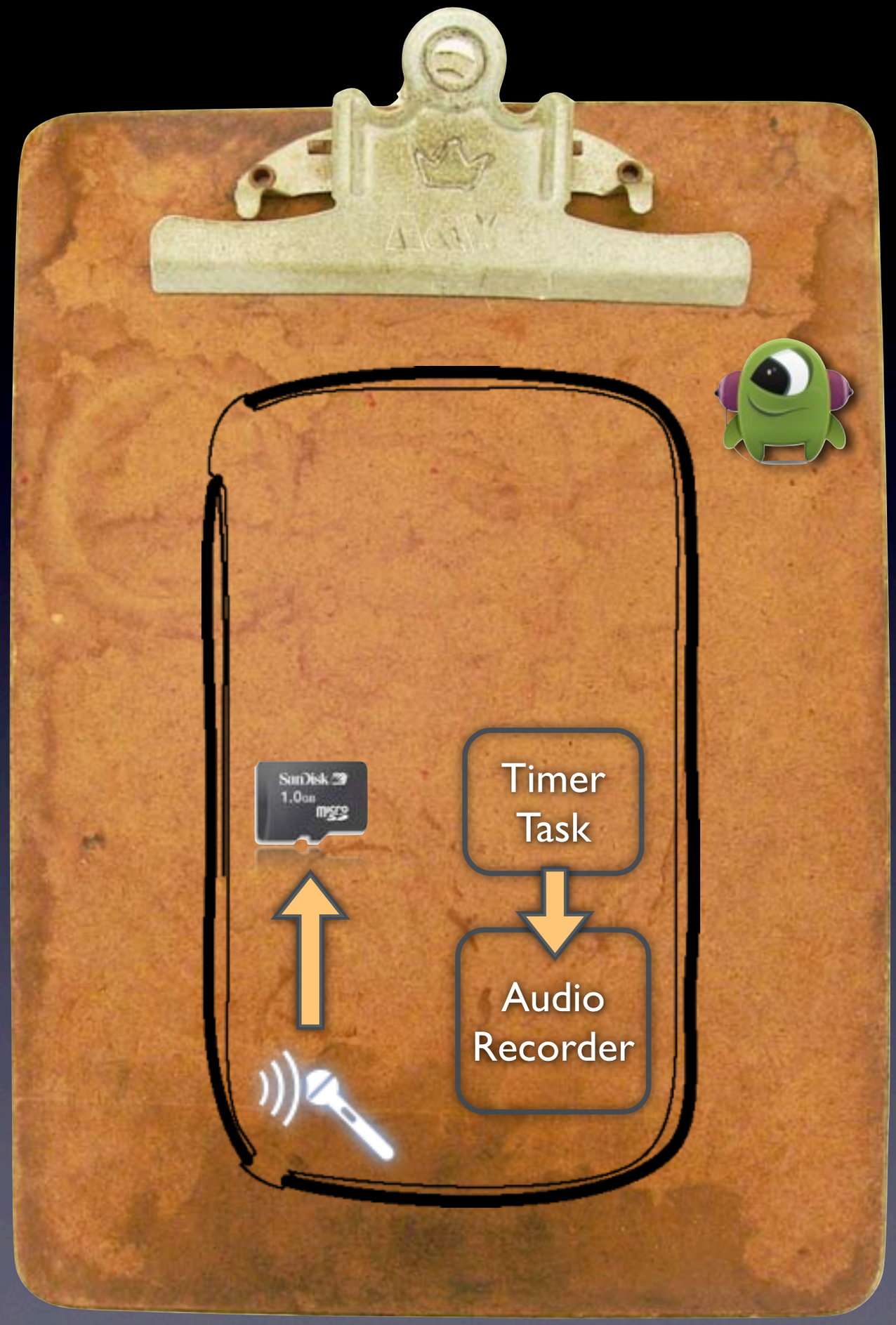
Interface: **Player / RecordControl**

Methods: **RecordControl.startRecord()**

- Switch on microphone at timed intervals and record ambient sounds

- Save to SD Card or Memory and extract periodically


BlackBerry


Timer
Task
Audio
Recorder

APIs

Camera

Package: **javax.microedition.media.control**

Interface: **VideoControl**

Methods: **getSnapshot()**

- Capture image from built-in camera

- Gives you a clue as to where the victim is

APIs

Location Based Services

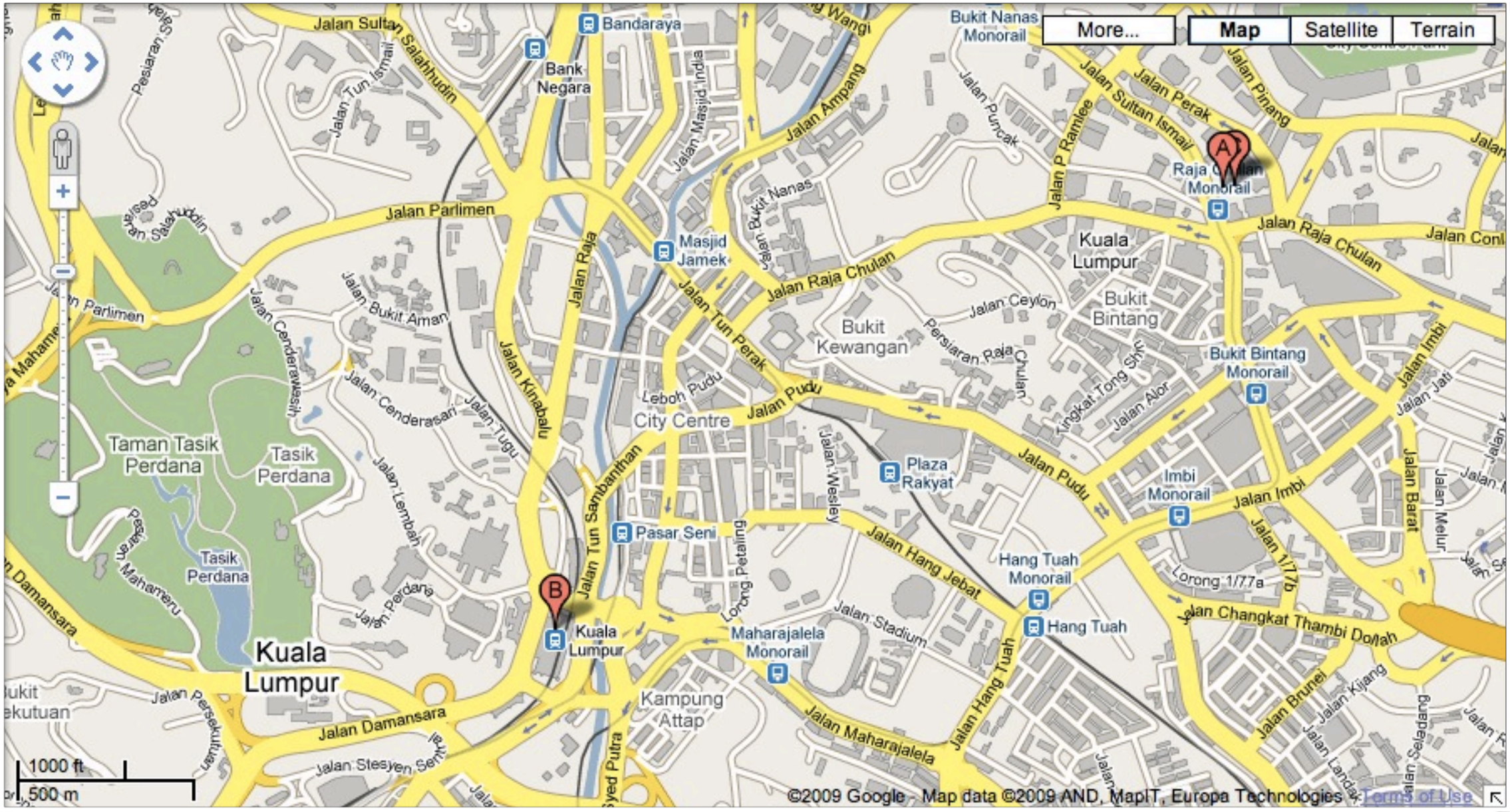
Package: **javax.microedition.location**

Class: **Location**

Methods: **getQualifiedCoordinates()**

- Track the location of the victim

- Either time based checking or trigger based


More...
Map
Satellite
Terrain
Bandaraya
Bank Negara
Jalan Sultan Salahuddin
Jalan Tun Ismail
Jalan Masjid India
Jalan Ampang
Bukit Nanas Monorail
Jalan Puncak
Jalan P Ramlee
Jalan Sultan Ismail
Jalan Perak
Jalan Pinang
Raja Chulan Monorail
Jalan Parlimen
Masjid Jamek
Jalan Bukit Nanas
Jalan Raja Chulan
Jalan Raja
Jalan Tun Perak
Kuala Lumpur
Bukit Kewangan
Jalan Ceylon
Bukit Bintang
Persiaran Raja Chulan
Bukit Bintang Monorail
Jalan Bukit Aman
Jalan Cenderawasih
Jalan Cenderasari
Jalan Tugu
Jalan Kinabalu
Leboh Pudu
City Centre
Jalan Pudu
Tingkat Tong Shin
Jalan Alor
Jalan Imbi
Jalan Jati
Taman Tasik Perdana
Tasik Perdana
Jalan Lembah
Plaza Rakyat
Imbi Monorail
Jalan Barat
Jalan Melur
Jalan Tun Sambanthan
Pasar Seni
Jalan Wesley
Jalan Hang Jebat
Hang Tuah Monorail
Lorong 1/77a
Jalan 1/77b
Jalan Changkat Thambi Dollah
Lorong Petaling
Jalan Stadium
Maharajalela Monorail
Hang Tuah
Jalan Hang Tuah
Jalan Damansara
Kampung Attap
Jalan Maharajalela
Jalan Brunei
Jalan Kijang
Jalan Perdana
Jalan Persekutuan
Jalan Stesyen Sentral
Syed Putra
1000 ft
500 m
©2009 Google - Map data ©2009 AND, MapIT, Europa Technologies
Terms of Use

BlackJacking

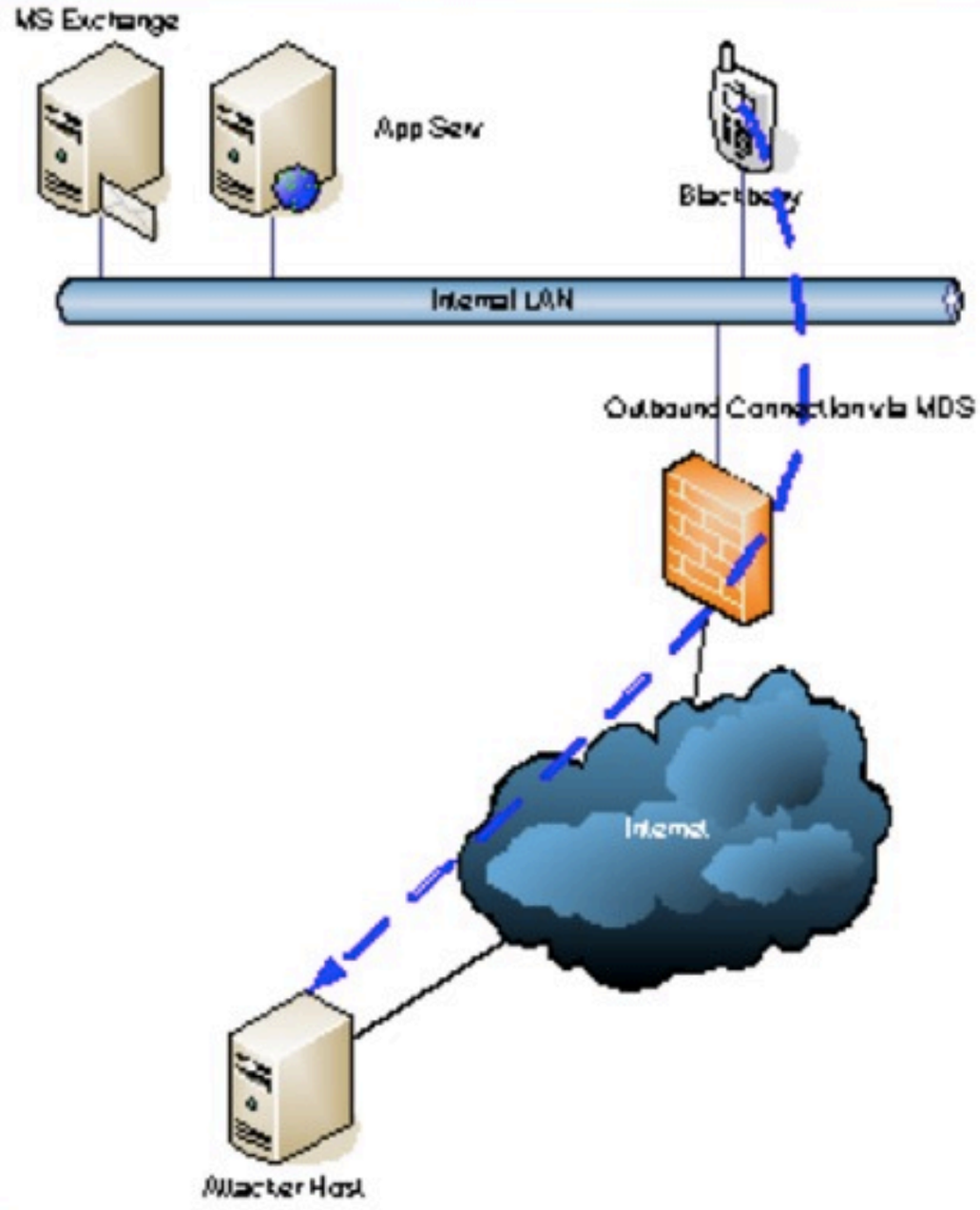
Attack Enterprise networks

Provide direct access to the internal network

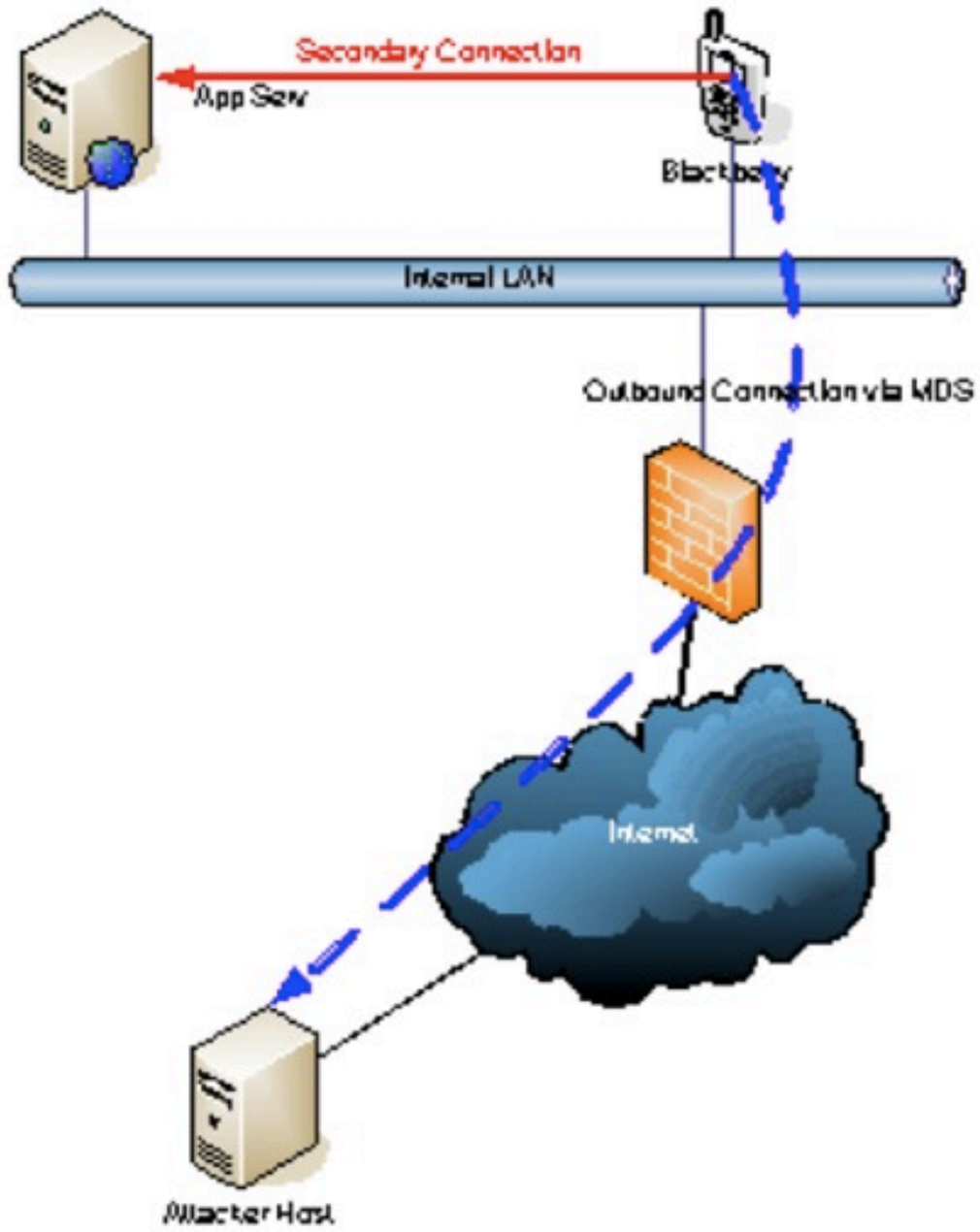
Use a BlackBerry to proxy connections

Tool released called BBProxy

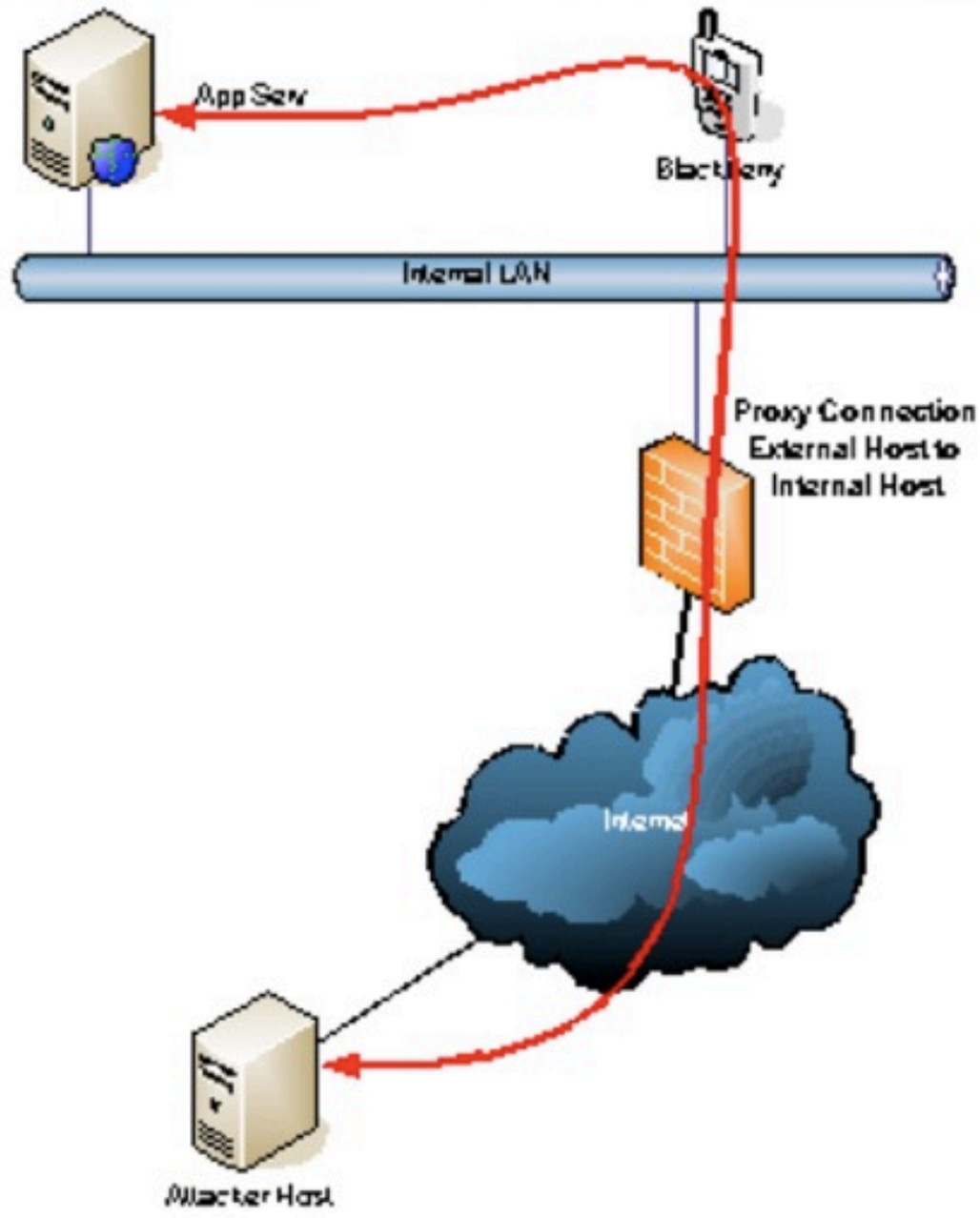
Step 1 – External Connection



Step 2 – Secondary Connection



Step 3 – Proxy connection between external and internal host



Other hacks

Steal contact information

Alter contact information, change email information, change meeting dates

Run up a victims phone bill by making international calls

Use victims phone to send bulk SMS messages

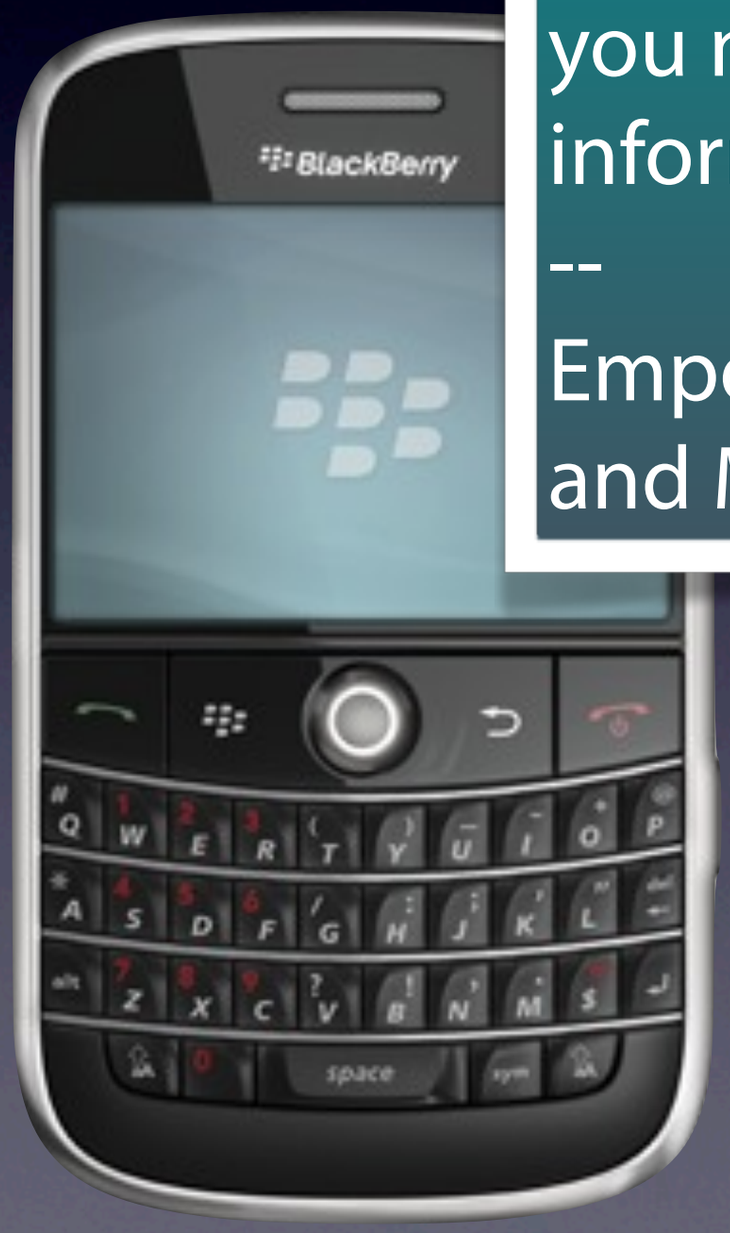
i can haz pwnage? kthx

Physically install the spyware on the device

Develop a game (too much work), or develop a simple slideshow with pr0n

Push a message indicating that the user should download an upgrade


etisalat



Dear Etisalat BlackBerry Customer,
Etisalat is always keen to provide you with the best BlackBerry service and ultimate experience, for that we will be sending you a performance enhancement patch that you need to install on your device. For more information, please call 101
--
Empower your Business with BlackBerry® and Mobile Solutions from Etisalat"

How did it work?

Hidden from Applications list

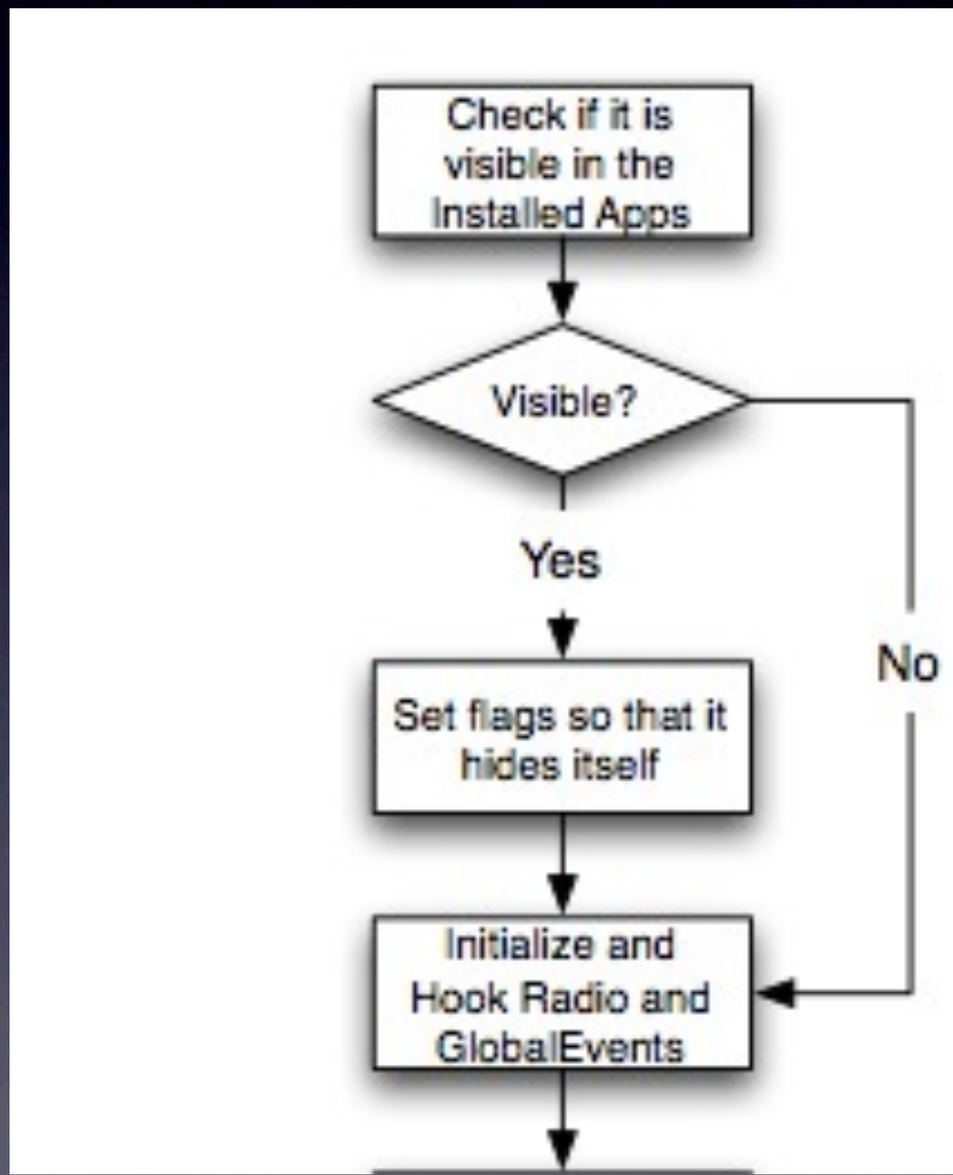
Starts off dormant

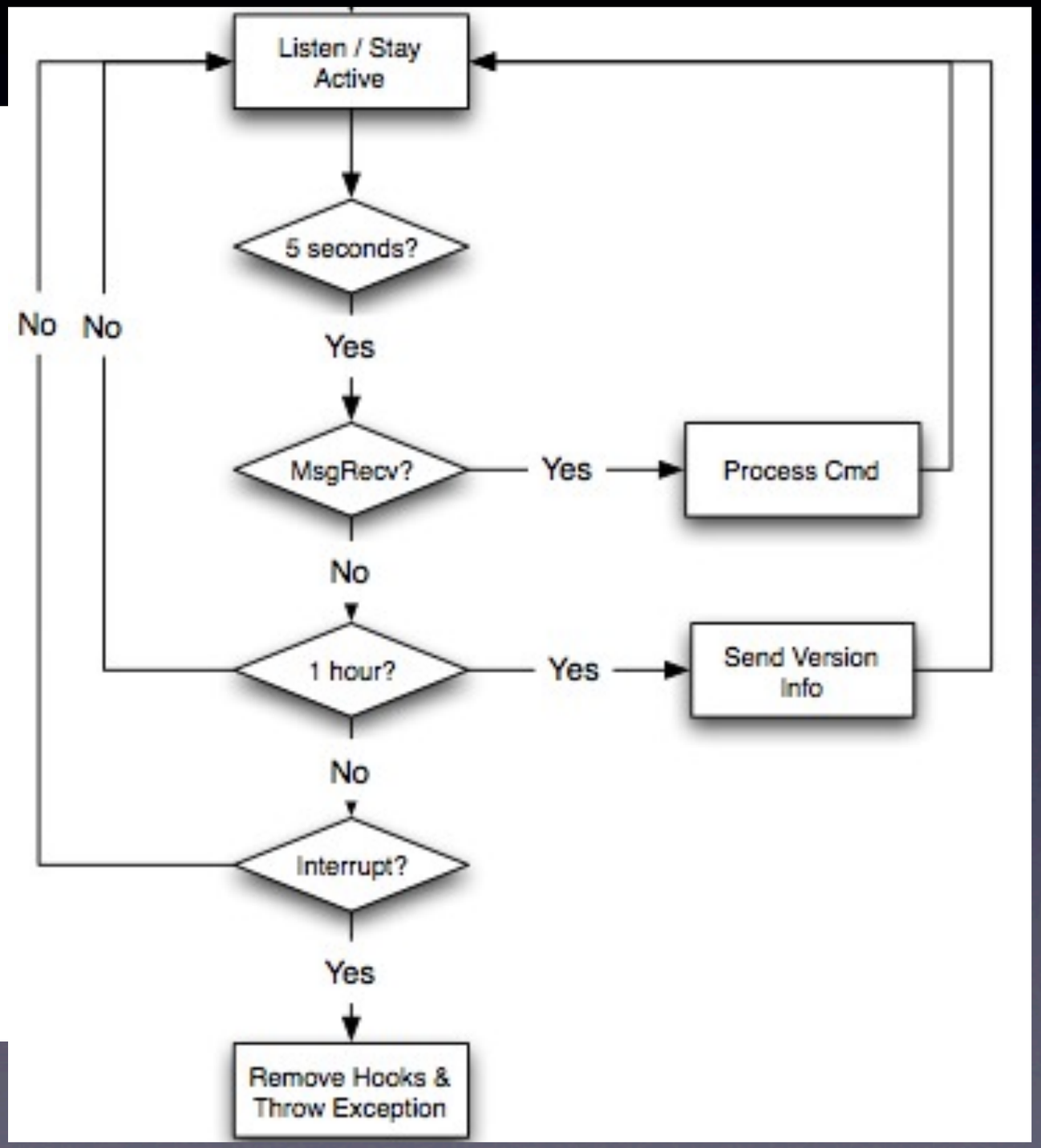
Has a command channel

Listens for message sent by “Customer Service”

Will forward all outgoing emails to a server

How did it work?





Problems

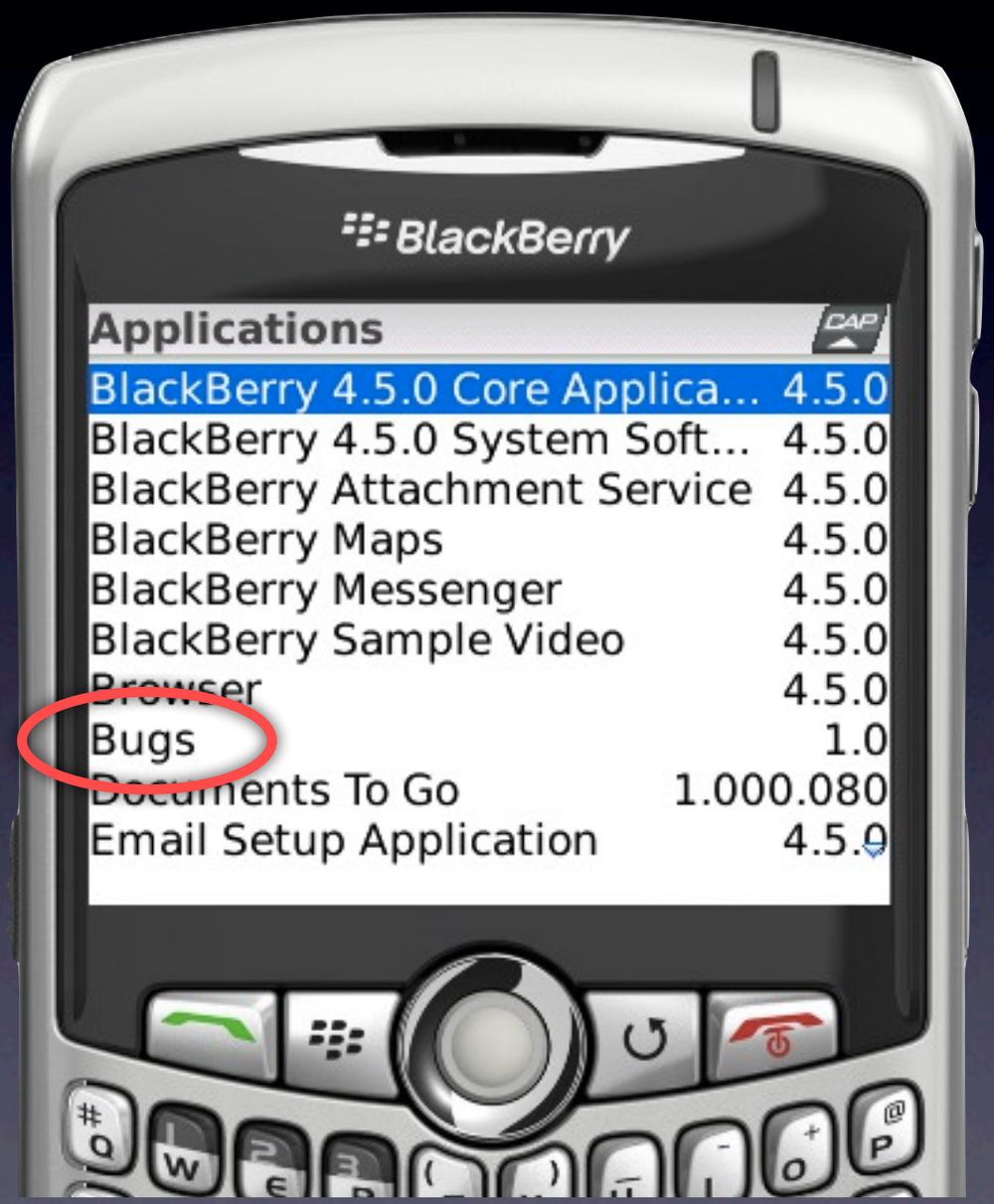
Constantly poll the message queue

Source code was available...sort of

Back end server collapsed

Berries slowed down, over heated and drained battery

How well hidden?



How well hidden?

```
CodeModuleGroup cmg =
CodeModuleGroupManager.load(“Bugs”);
cmg.setFlag
(CodeModuleGroup.FLAG_HIDDEN,true);
```

Kisses

Finds Bugs & other similar, hidden software

Simplifies the search for hidden apps.

Version 2.0 will be out next week!

Download:

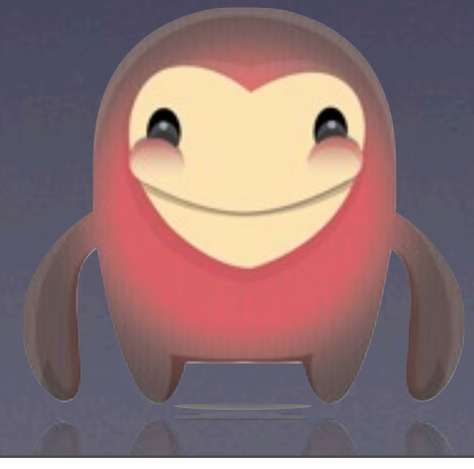
http://www.zensay.com/Kisses.jad

Kisses

Works on Signature based detection

Allows a user to submit phone data for analysis

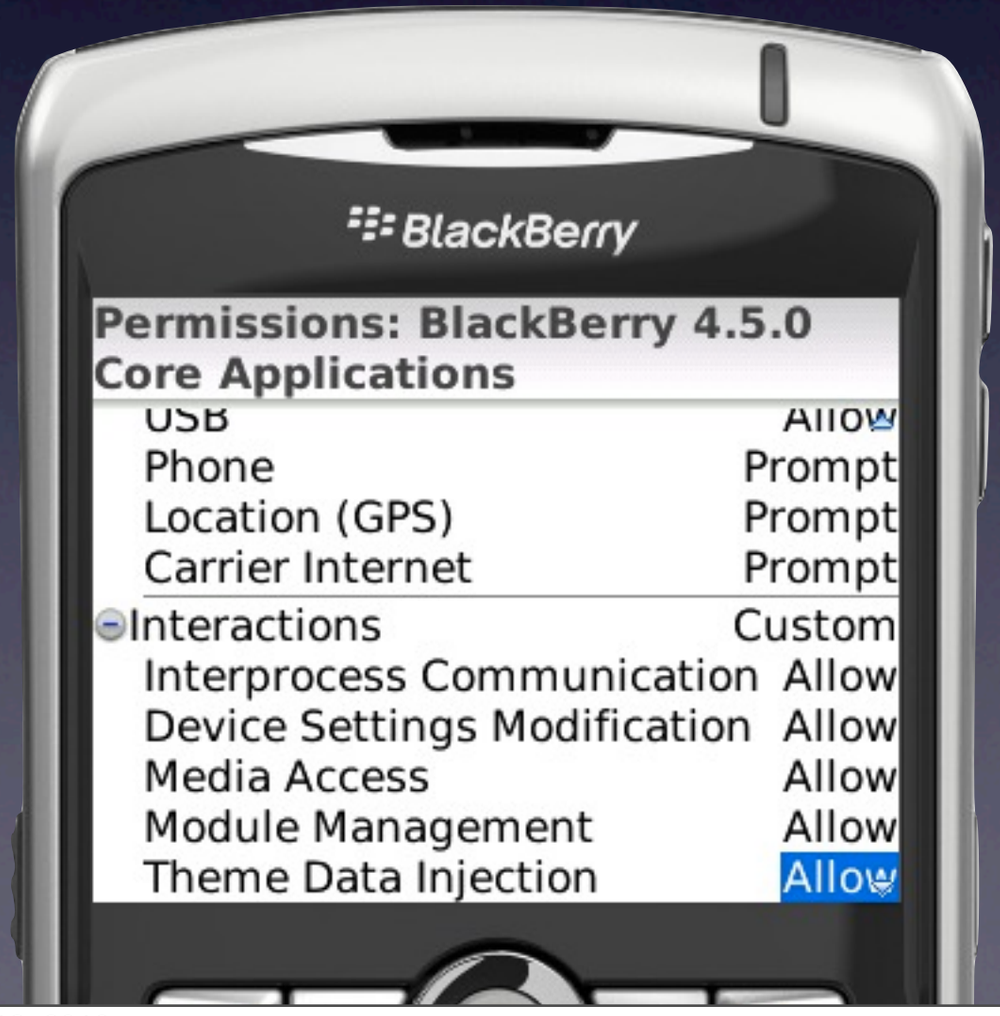
Baseline analysis is performed

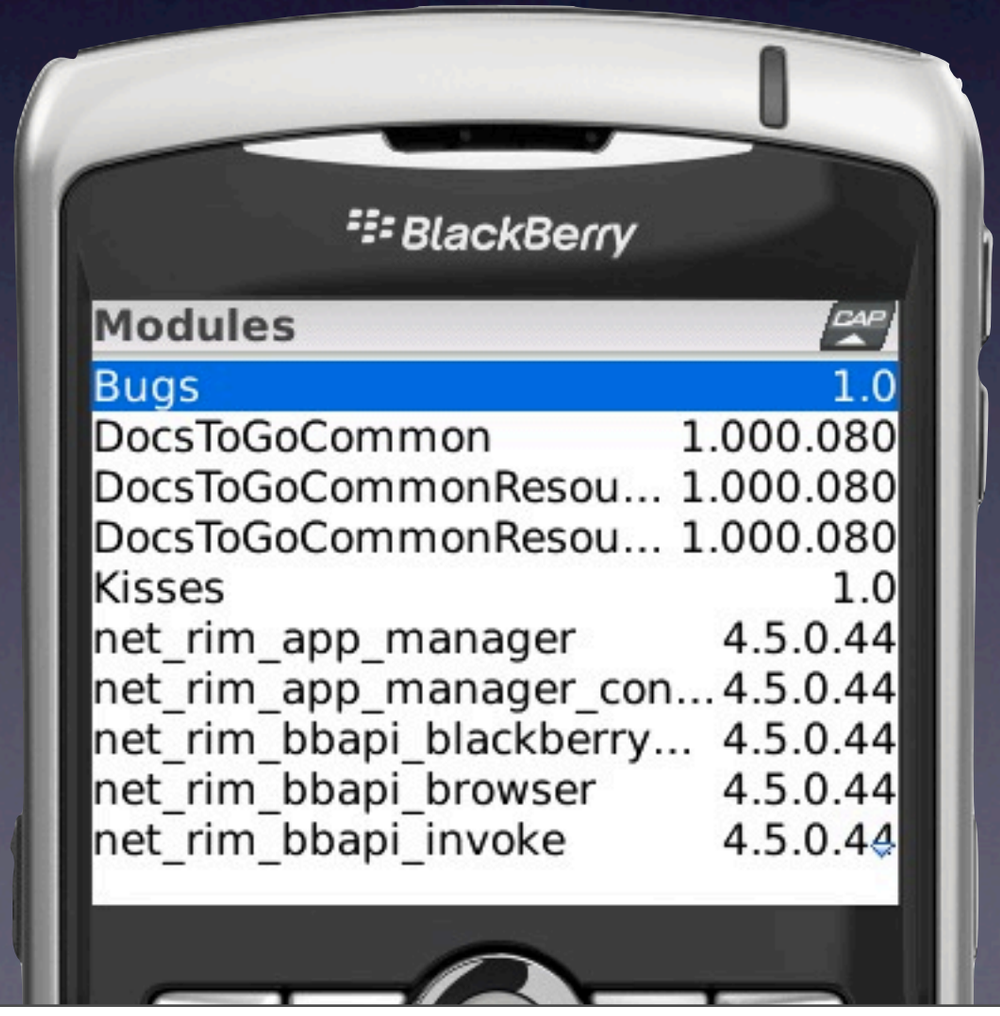


Wrapping up

The BlackBerry is very secure

The problem lies in its complexity





Wrapping up

BlackBerry apps are not regulated

Nothing between you & spyware

Watch out

Don’t install random pieces of software

Limit the amount of software on your BB

Learn and set Default Application Permissions

Don’t let others use your phone

Always enable a device password

Keep up to date

http://chirashi.zensay.com

@chopstick_

Questions?

Thank you

ERNW
Living Security.