Bugs & Kisses

Spying on BlackBerry users for fun

HITB Security Conference, Malaysia 2009

Social Engineering

Social Engineering

The clever manipulation of the natural human tendency to trust.

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.

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

Wednesday, October 7, 2009

Wednesday, October 7, 2009


BlackBerry
space

Push Email

QWERTY Keyboard

Granular Security Controls

Transport Level Security

Device Encryption

Granular Controls

Granular Controls

Allow or deny access to User Data

Granular Controls

Allow or deny access to User Data

Allow or deny access to Application Interaction

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 mini-SD card cannot be read on another device

Stolen, encrypted devices are still safe

Granular Security Controls

Transport Level Security

Device Encryption

Vulnerabilities on SecurityFocus - Sep ’09

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

A Few Problems

We can’t hack it - no useful vulnerabilities

A Few Problems

We can’t hack it - no useful vulnerabilities

We can’t MITM - everything is encrypted

A Few Problems

We can't hack it - no useful vulnerabilities

We can't MITM - everything is encrypted

We could steal it...

APIs

DTMF Tones

Upto version 4.3.0: **getDTMFTones()**

- Grabs DTMF Tones from the Call Queue

After 4.3.0: **addKeyListener(), keyDown(), keyUp(), keyStatus()**

- Install a Key Logger

APIs

Text Messages

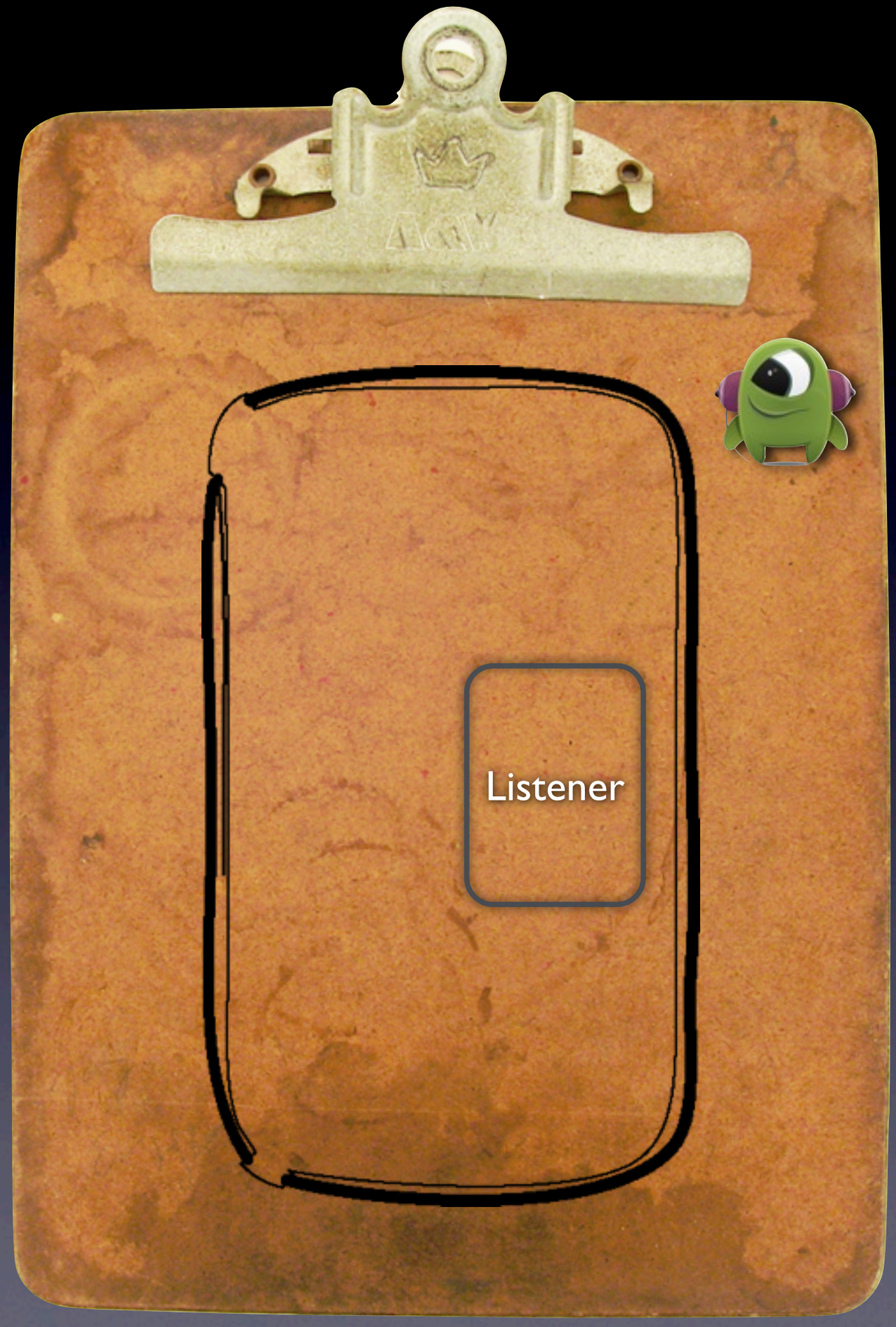
Package: **javax.wireless.messaging**

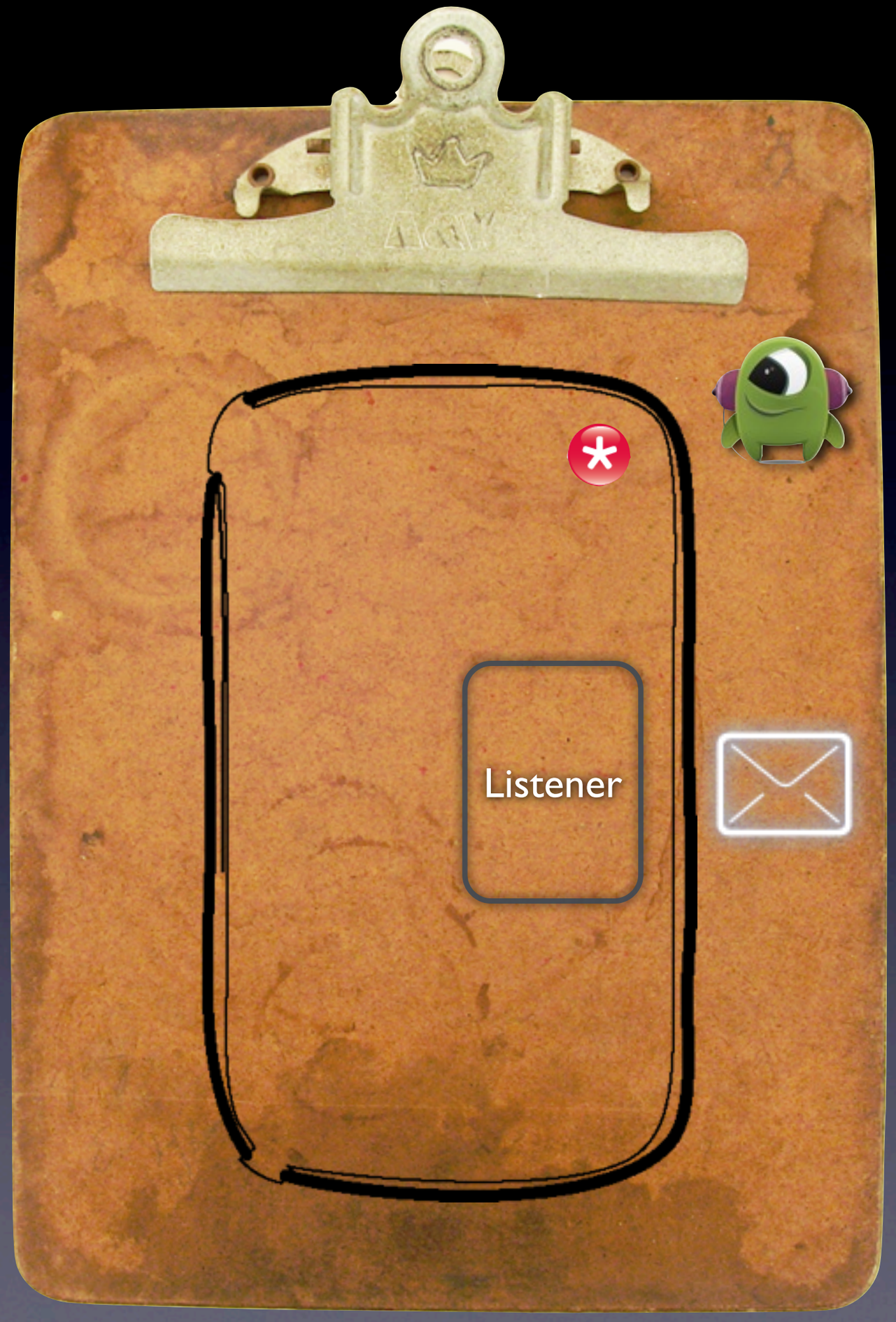
Interface: **MessageListener**

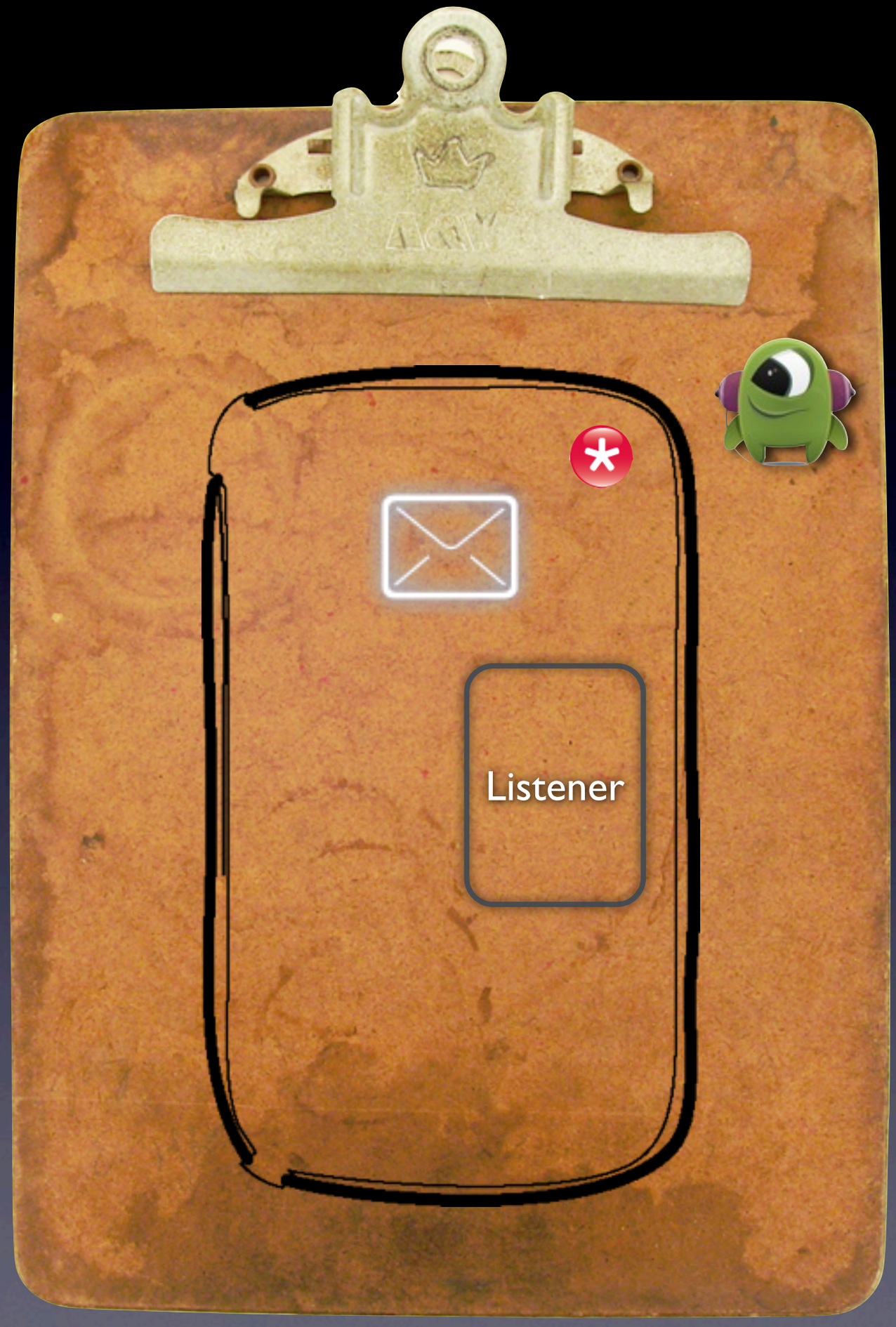
Methods: **setMessageListener()**

- Receive and Send SMS messages without owner's knowledge


BlackBerry
space


Listener


Listener


Listener

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**

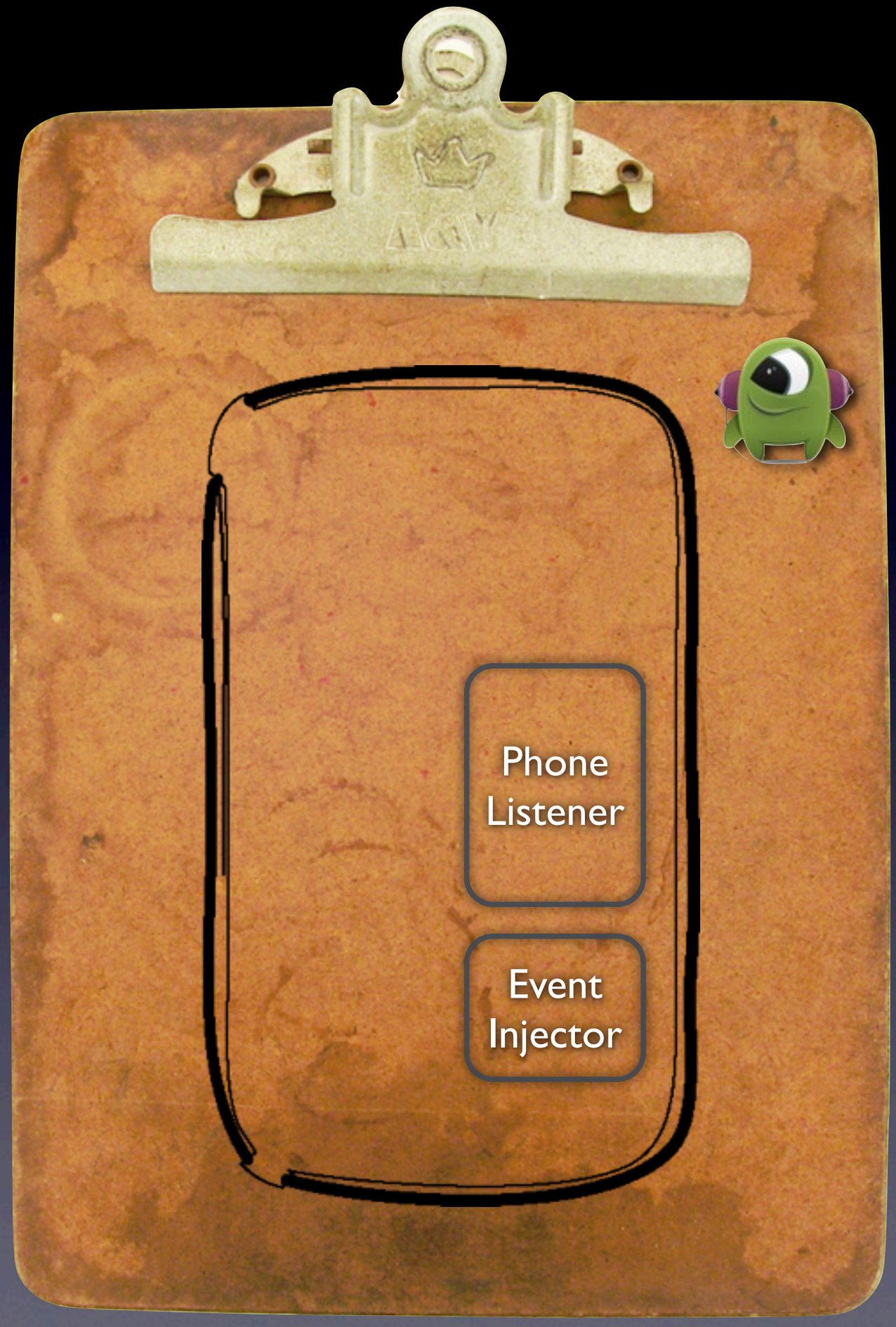
Interface: **PhoneListener**

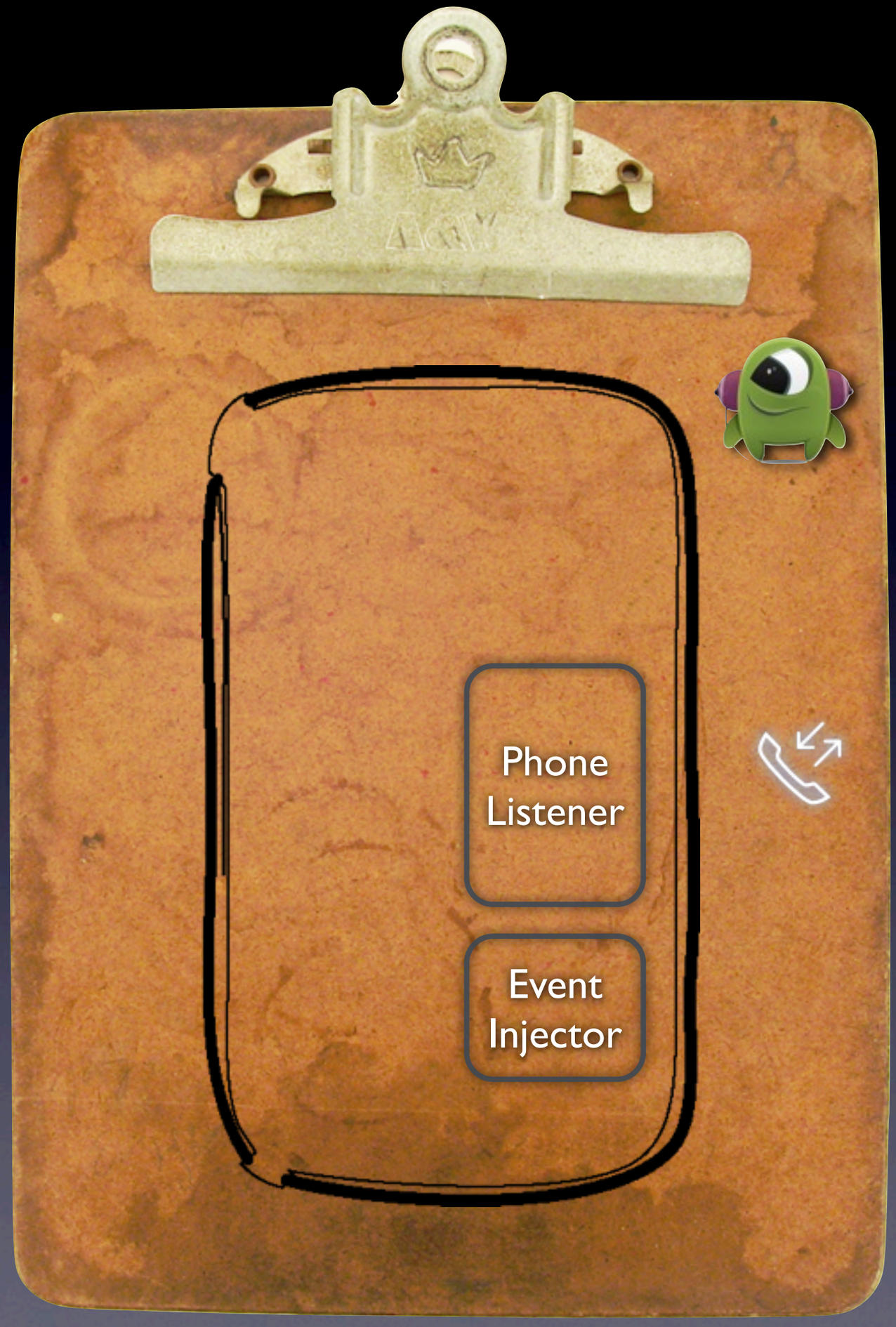
Methods: **EventInjector.invokeEvent()**

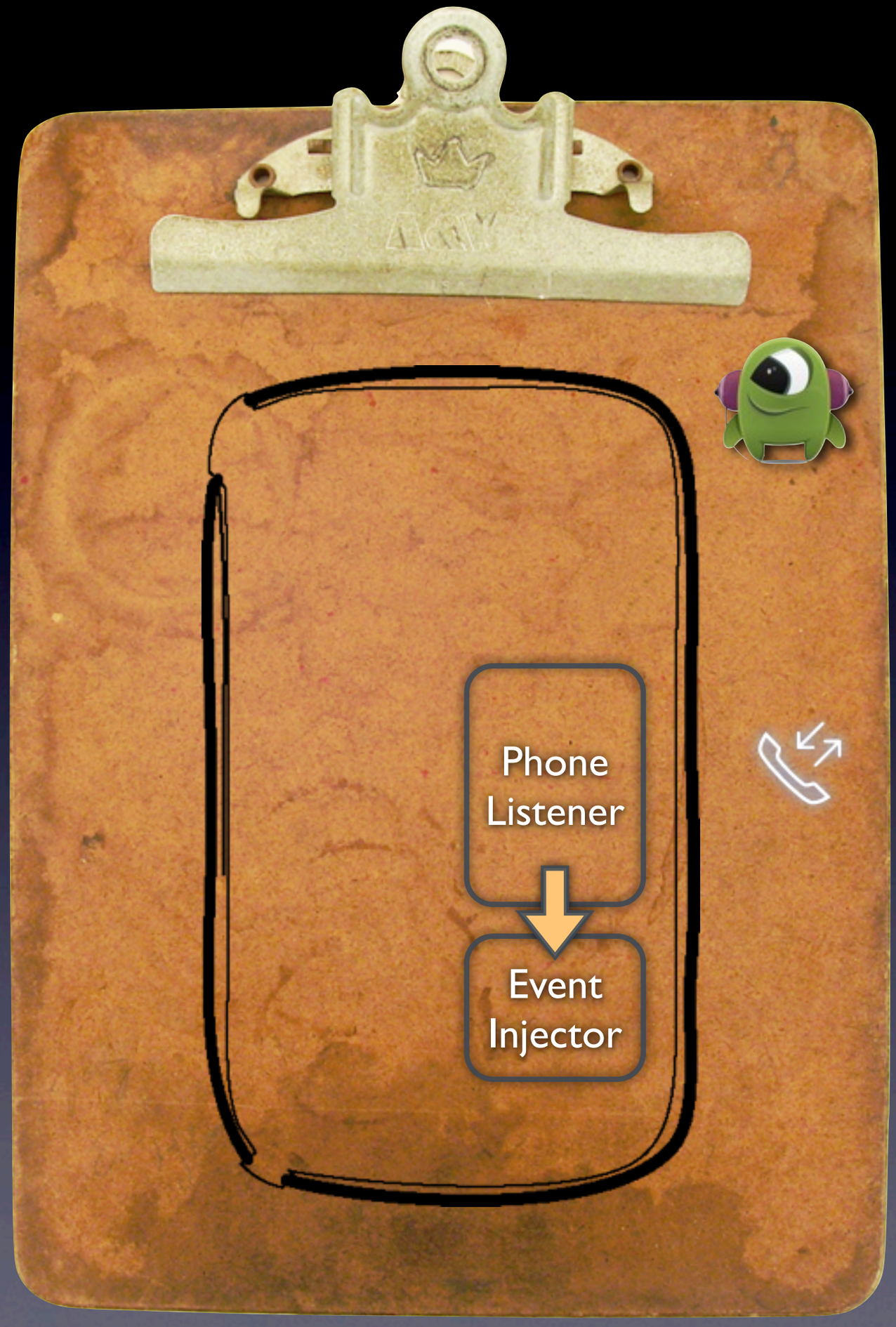
- Silently intercept phone call, turn microphone on and listen in

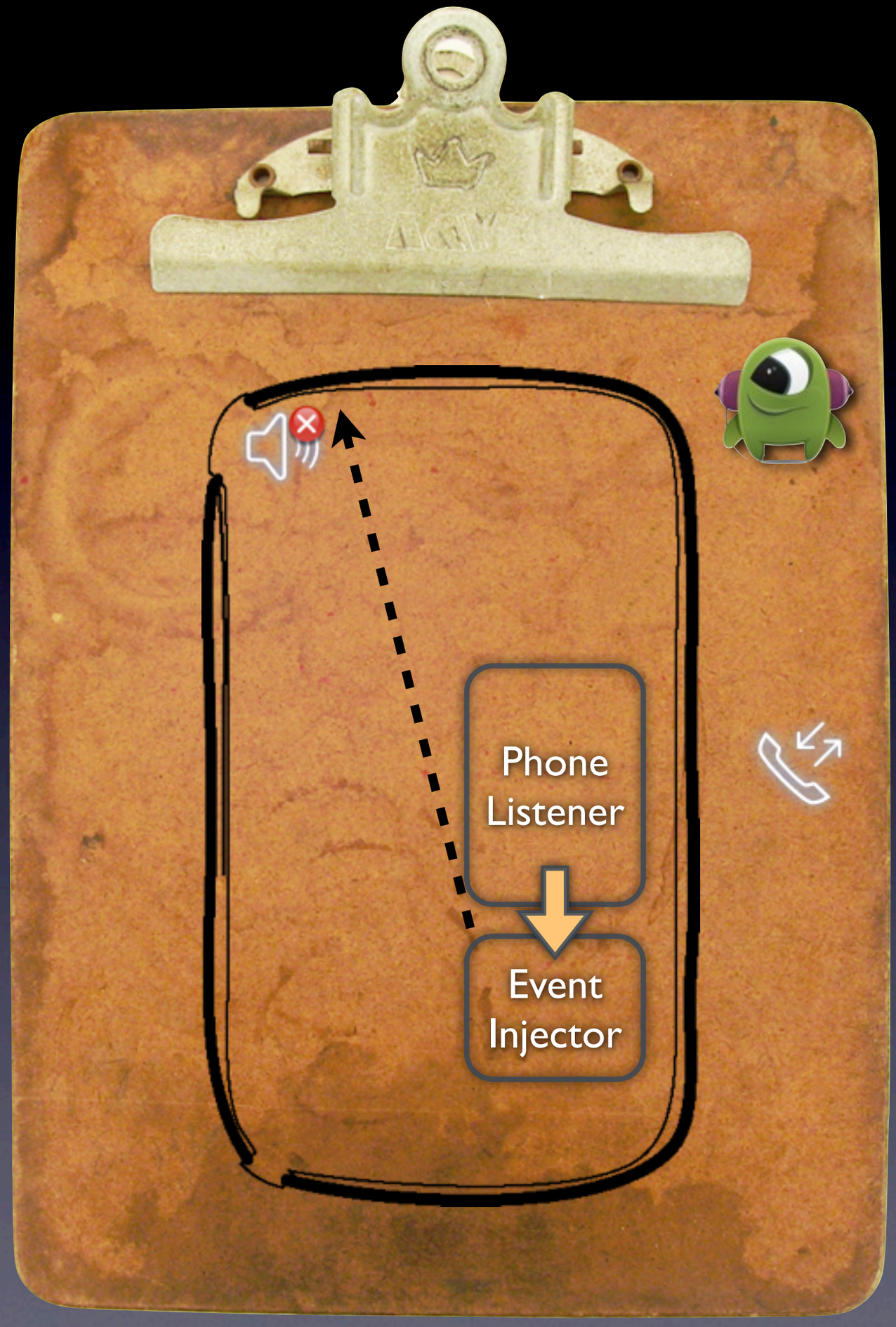
- Portable bugging device

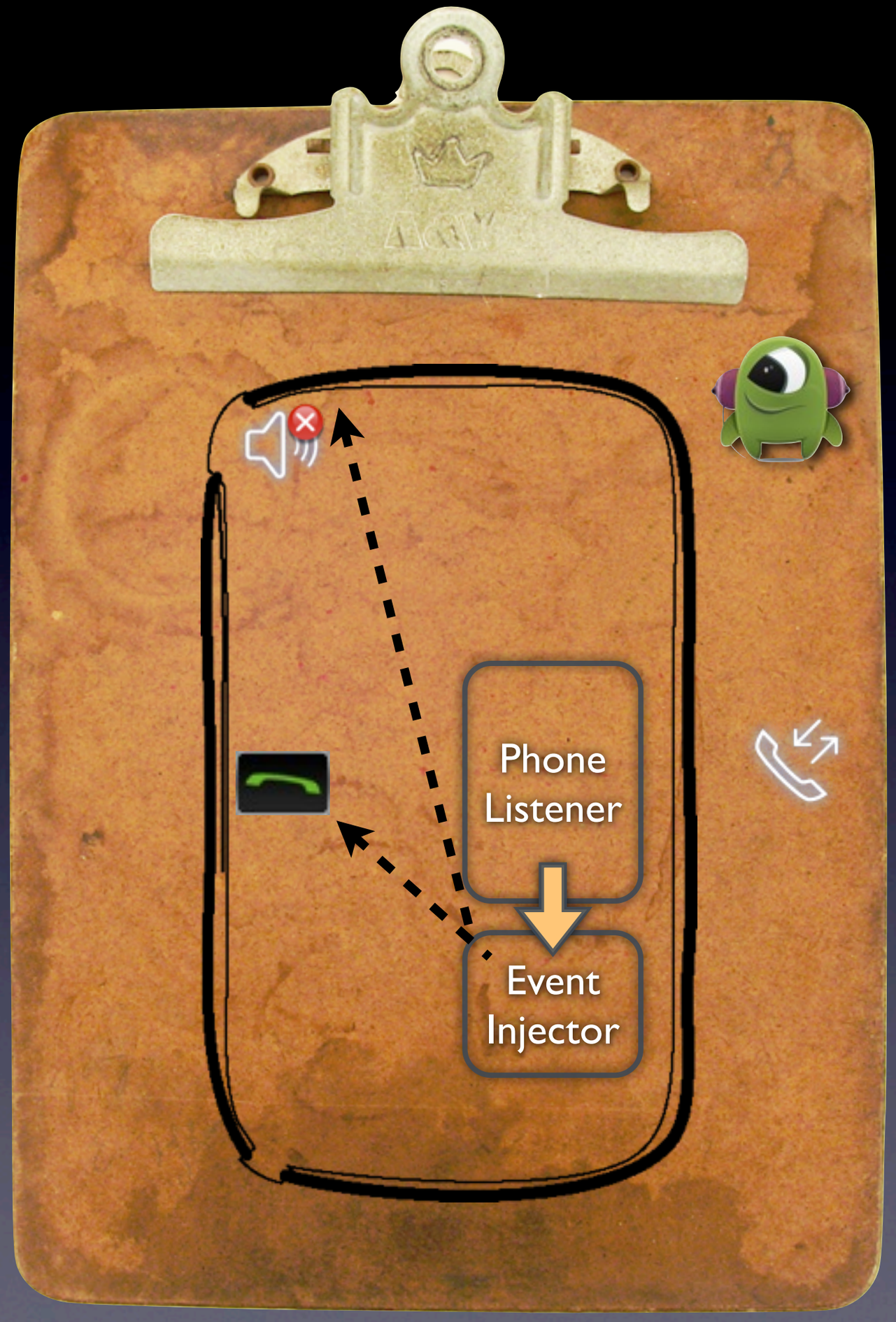

BlackBerry
space

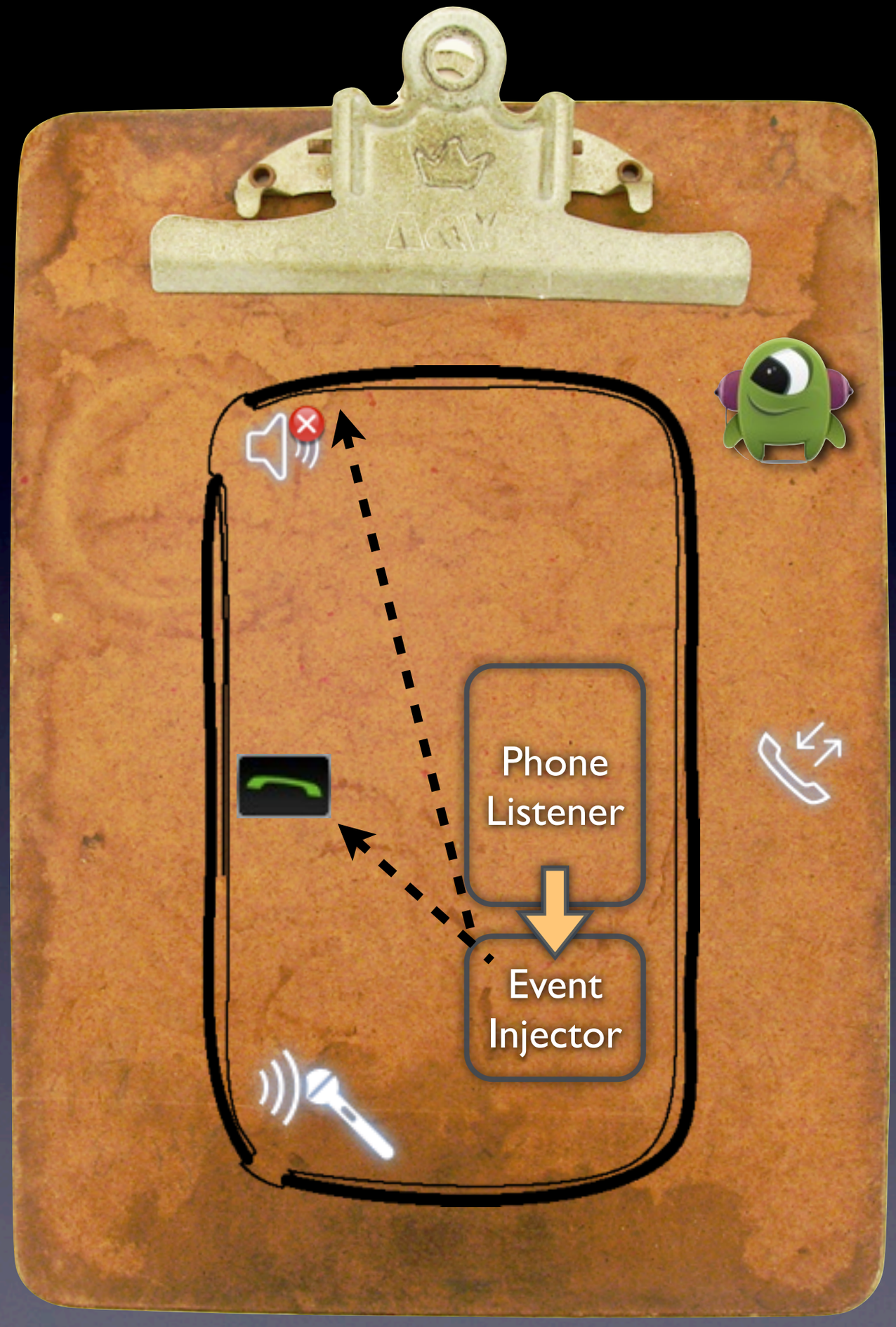

Phone
Listener
Event
Injector


Phone
Listener
Event
Injector


Phone
Listener
Event
Injector


Phone
Listener
Event
Injector


Phone
Listener
Event
Injector


Phone
Listener
Event
Injector

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

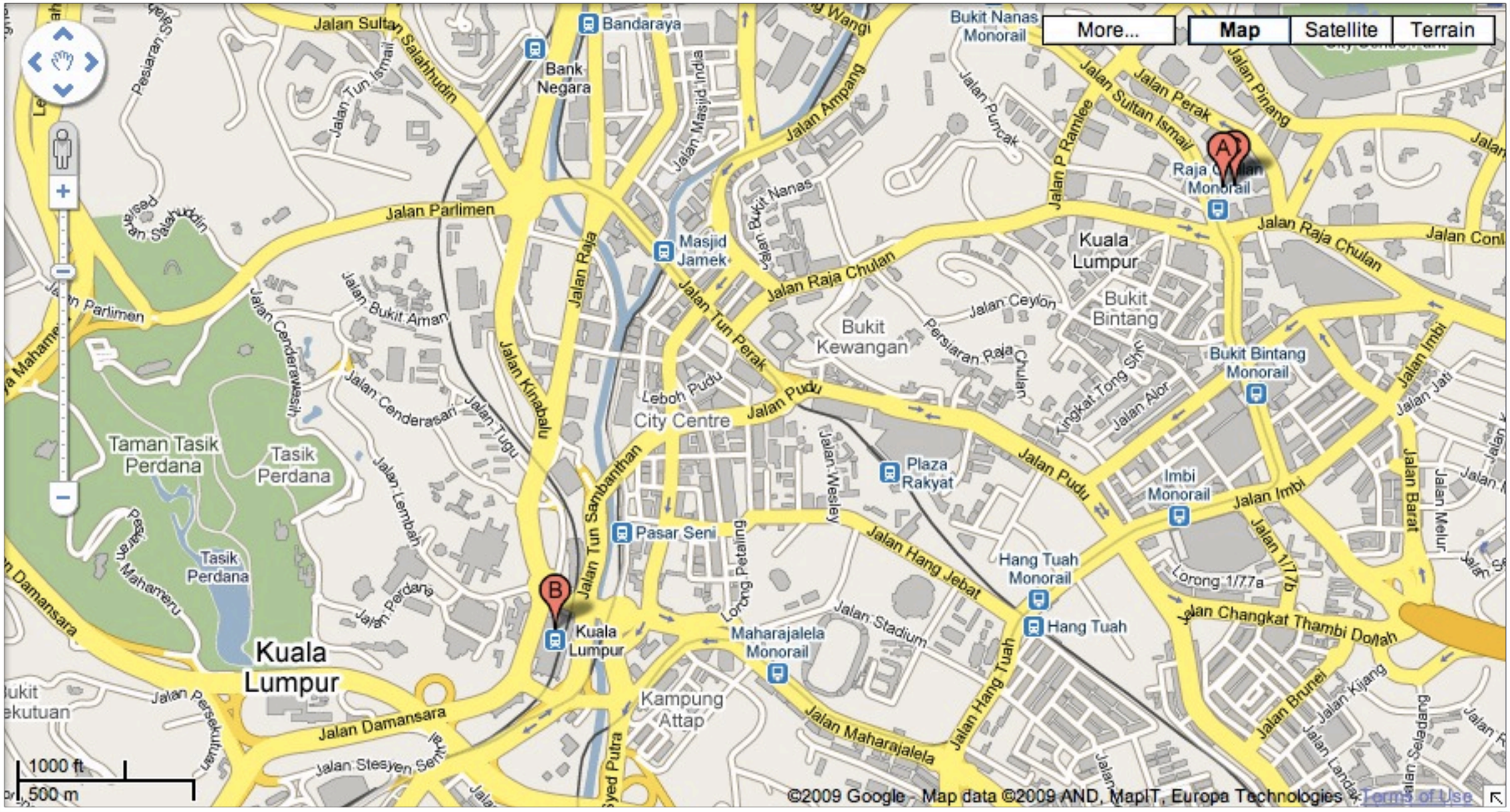
Package: **javax.microedition.location**

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
Kuala Lumpur
Jalan Tun Perak
Jalan Ceylon
Bukit Bintang
Bukit Kewangan
Persiaran Raja Chulan
Bukit Bintang Monorail
Jalan Cenderawasih
Jalan Bukit Aman
Jalan Kinabalu
Jalan Raja
Jalan Cenderasari
Jalan Tugu
Leboh Pudu
City Centre
Jalan Pudu
Jalan Alor
Jalan Imbi
Taman Tasik Perdana
Tasik Perdana
Plaza Rakyat
Imbi Monorail
Jalan Lembah
Jalan Tun Sambanthan
Pasar Seni
Jalan Wesley
Jalan Hang Jebat
Hang Tuah Monorail
Lorong 1/77a
Jalan Perdana
Lorong Petaling
Jalan Stadium
Hang Tuah
Jalan Changkat Thambi Dollah
Kuala Lumpur
Maharajalela Monorail
Jalan Hang Tuah
Jalan Damansara
Kampung Attap
Jalan Maharajalela
Jalan Brunei
Jalan Kijang
1000 ft
500 m
©2009 Google - Map data ©2009 AND, MapIT, Europa Technologies
Terms of Use

BlackJacking

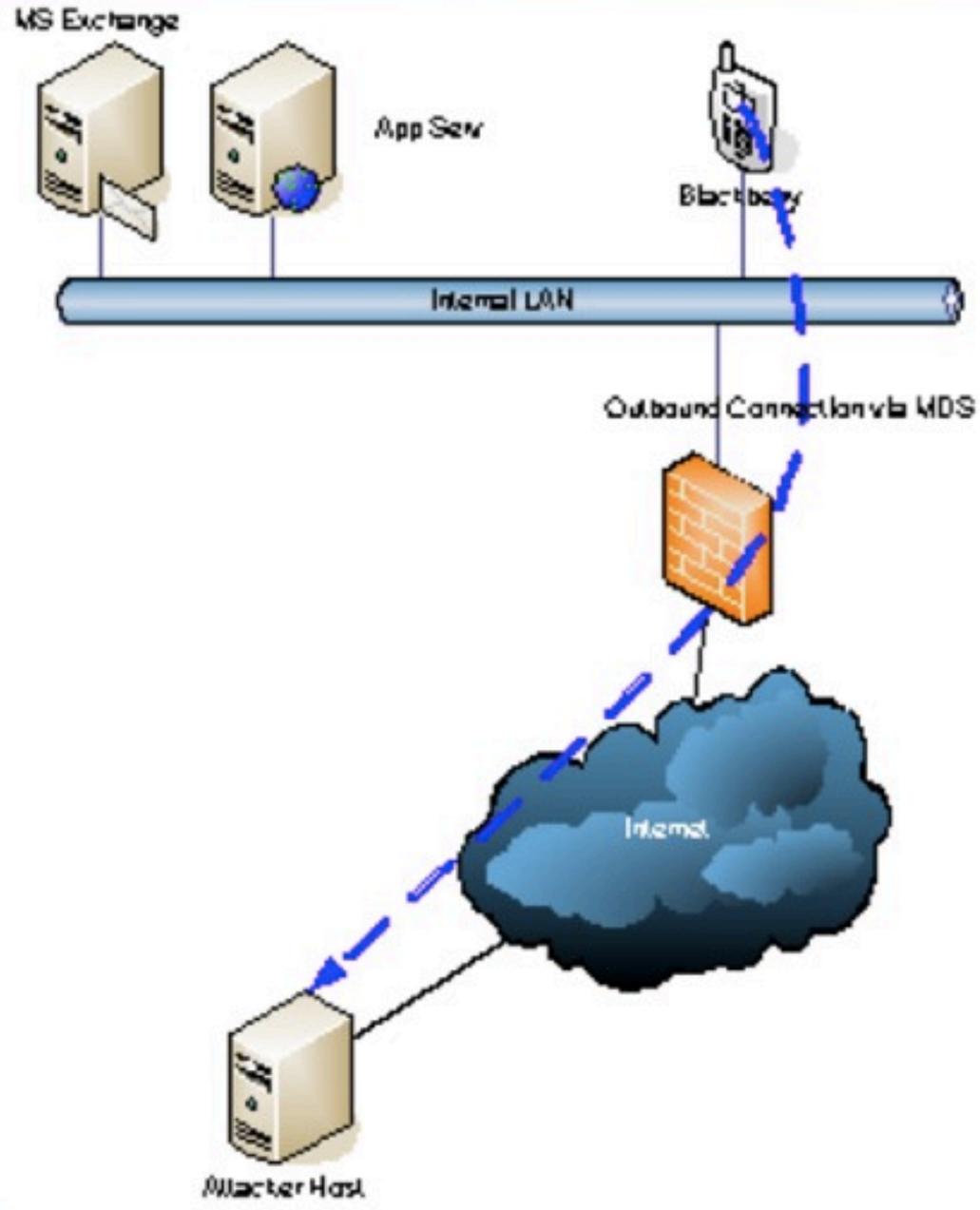
Attack Enterprise networks

Provide direct access to the internal network

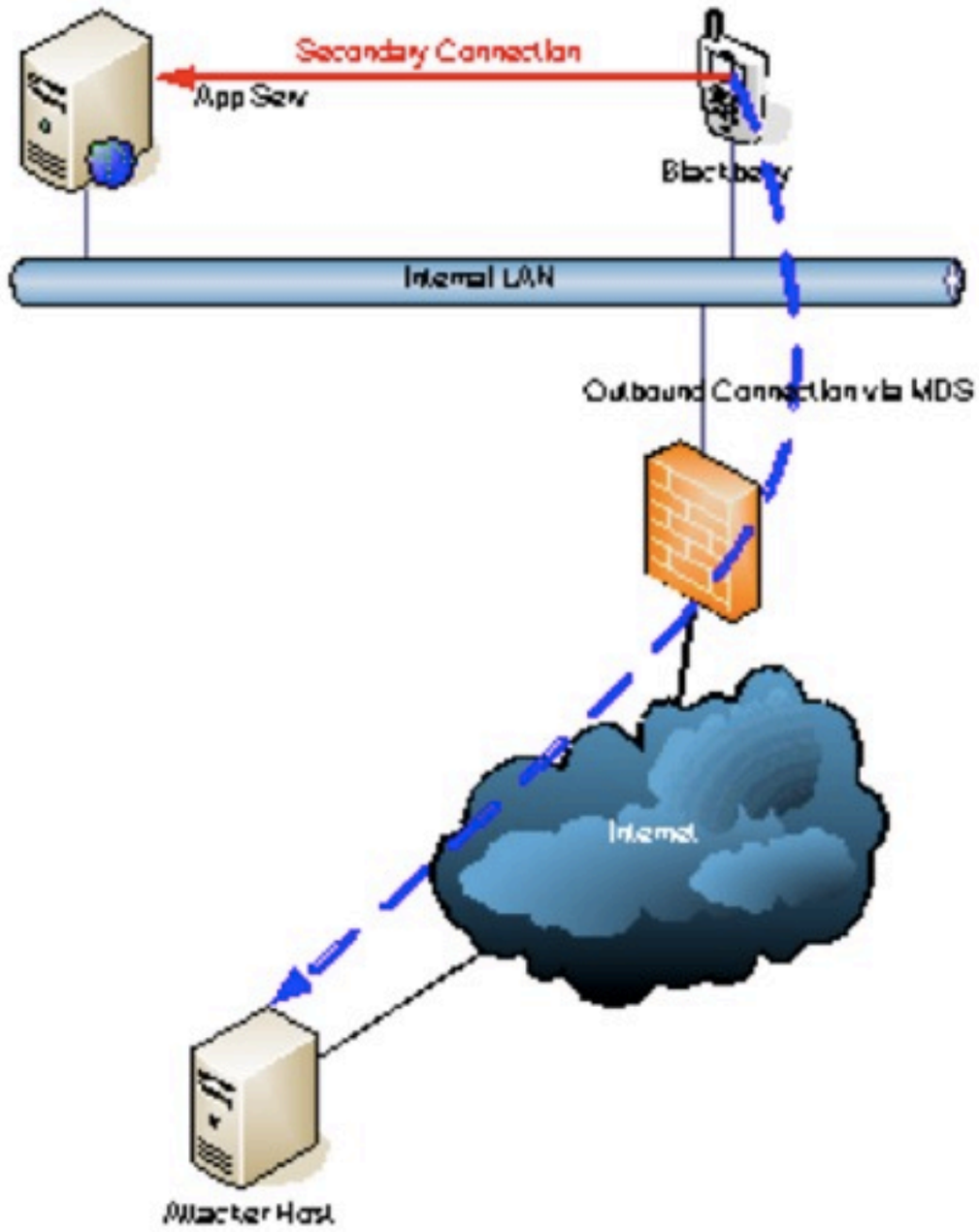
Use a BlackBerry to proxy connections

Tool released called BBProxy

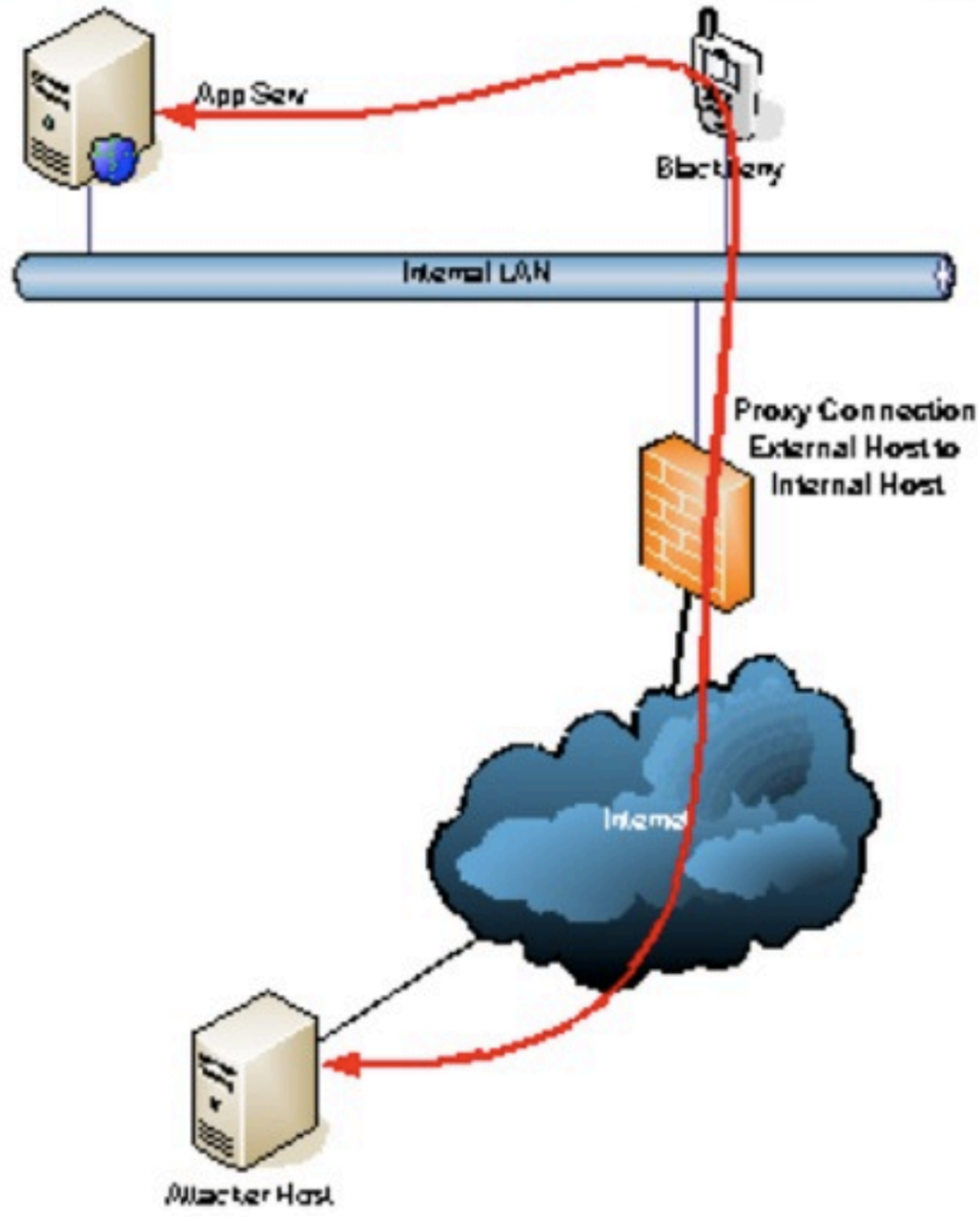
Step 1 – External Connection



Step 2 – Secondary Connection



Step 3 – Proxy connection between external and internal host



Other hacks

Other hacks

Steal contact information

Other hacks

Steal contact information

Alter contact information, change email information, change meeting dates

Other hacks

Steal contact information

Alter contact information, change email information, change meeting dates

Run up a victims phone bill by making international calls

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

i can haz pwnage? kthx

Physically install the spyware on the device

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

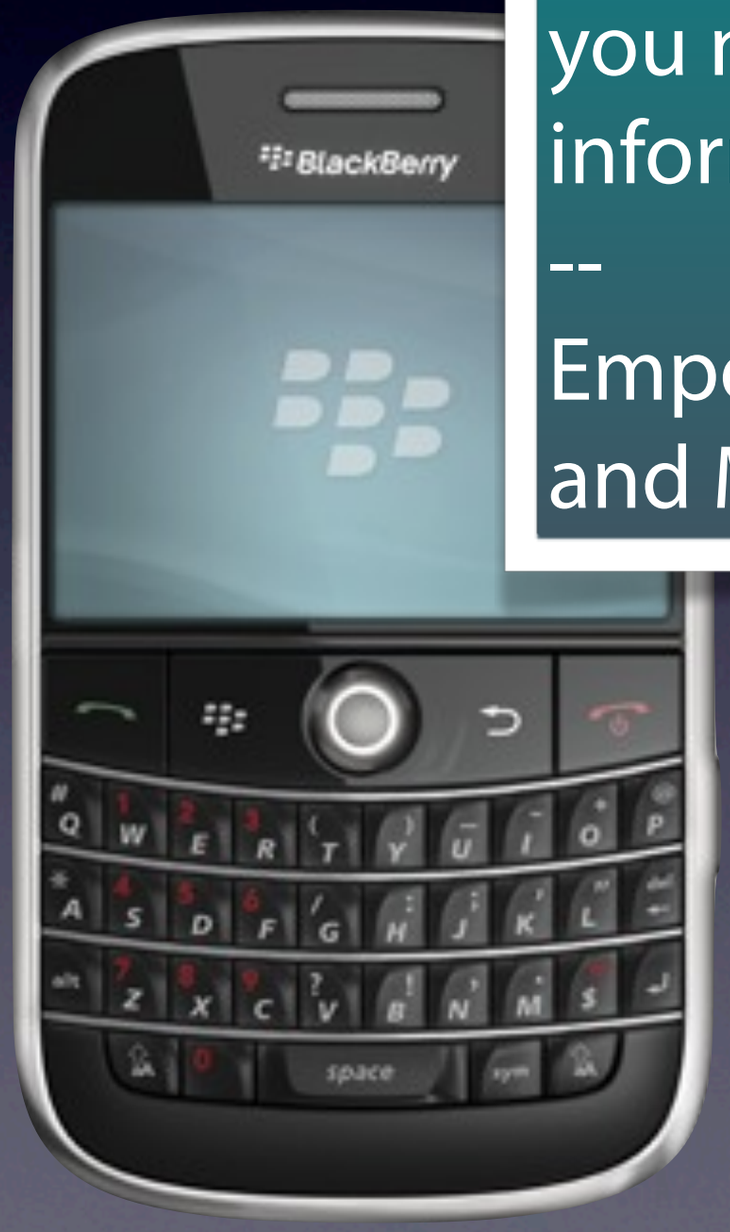
i can haz pwnage? kthx

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?

Starts off dormant

Has a command channel

Listens for message sent by “Customer Service”

Will forward all outgoing emails to a server

Problems

Problems

Constantly poll the message queue

Problems

Constantly poll the message queue

Source code was available...sort of

Problems

Constantly poll the message queue

Source code was available...sort of

Back end server collapsed

Problems

Constantly poll the message queue

Source code was available...sort of

Back end server collapsed

Berries slowed down, over heated and drained battery

Demo

Bugs

Bugs

Spyware that sniffs messages, keystrokes, voice and location

Bugs

Spyware that sniffs messages, keystrokes, voice and location

Today: Only sniffs email

Bugs

Spyware that sniffs messages, keystrokes, voice and location

Today: Only sniffs email

Working prototype of voice bug

Bugs

Spyware that sniffs messages, keystrokes, voice and location

Today: Only sniffs email

Working prototype of voice bug

Tries to be stealthy by hiding from apps. (not for this demo)

Bugs

Forwards all mail to charlie@zensay.com

Download:

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

Email from Bugs

Inbox | X

Sheran Gunasekera <?xml version="1.0"?> <Message><Type>Inbound</Type><Sender>mailto:workingadva... 2:33 AM (8 hours ago)

Sheran Gunasekera <?xml version="1.0"?> <Message><Type>Inbound</Type><Sender>mailto:sheran@zens... 6:03 AM (4 hours ago)

Sheran Gunasekera to me show details 6:33 AM (4 hours ago) Reply ▾

<?xml version="1.0"?>
<Message><Type>Inbound</Type><Sender>mailto:calendar-notification@google.com</Sender><Recipients><To>sheran.g@hermisconsulting.com</To></Recipients><Subject>You have no events scheduled today.</Subject><Body>sheran.g@hermisconsulting.com,Â you have no events scheduled today Wed Oct 7, 2009
You are receiving this email at the account sheran.g@hermisconsulting.com because you are subscribed to receive daily agendas for the following calendars:
Sheran Gunasekera.
To change which calendars you receive daily agendas for, please log in to http://www.google.com/calendar/hosted/hermisconsulting.com/ and change your notification settings for each calendar.
</Body><Date>Wed Oct 07 06:33:30 Asia/Kuala_Lumpur 2009</Date></Message>

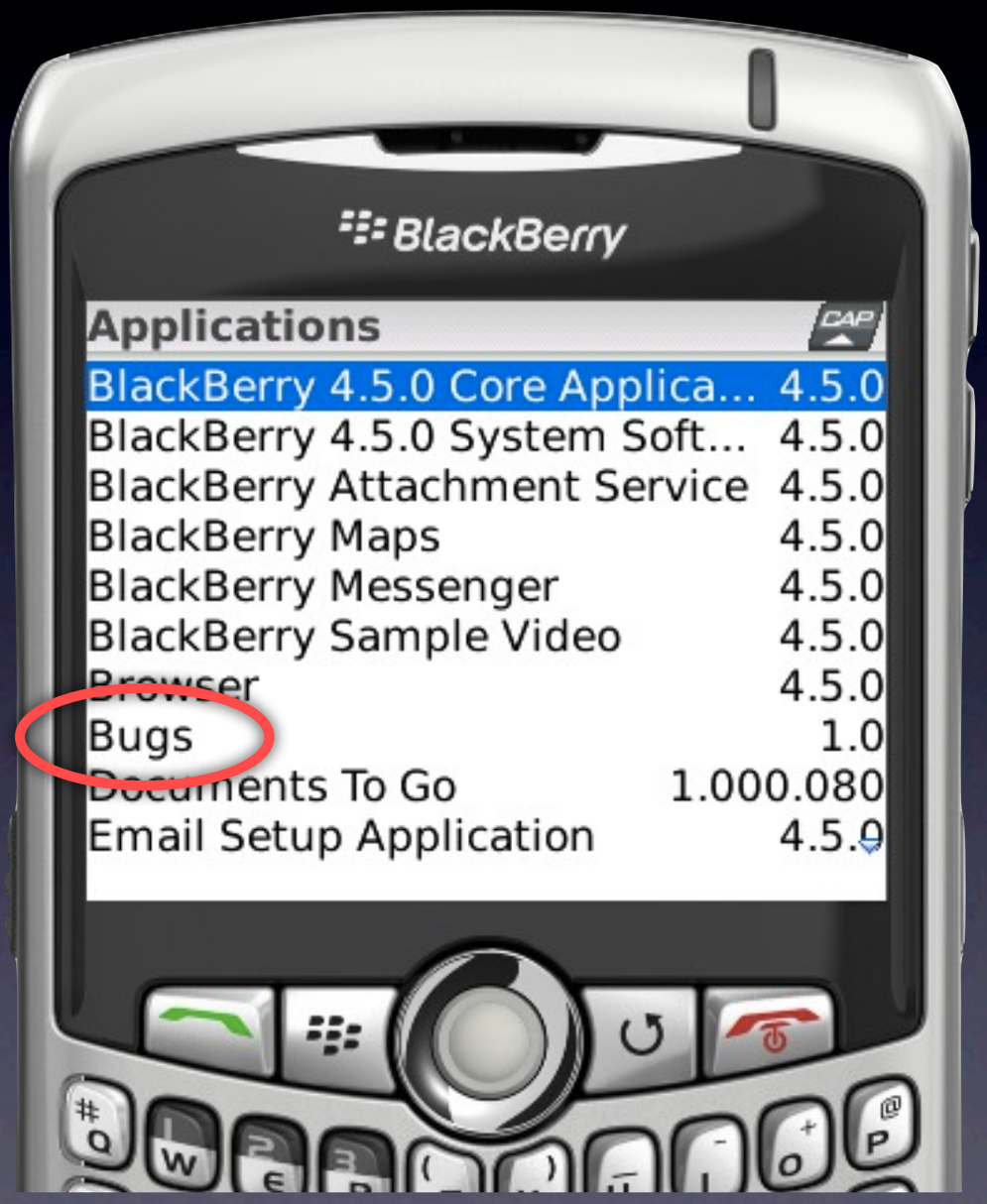
Reply Forward

Bugs

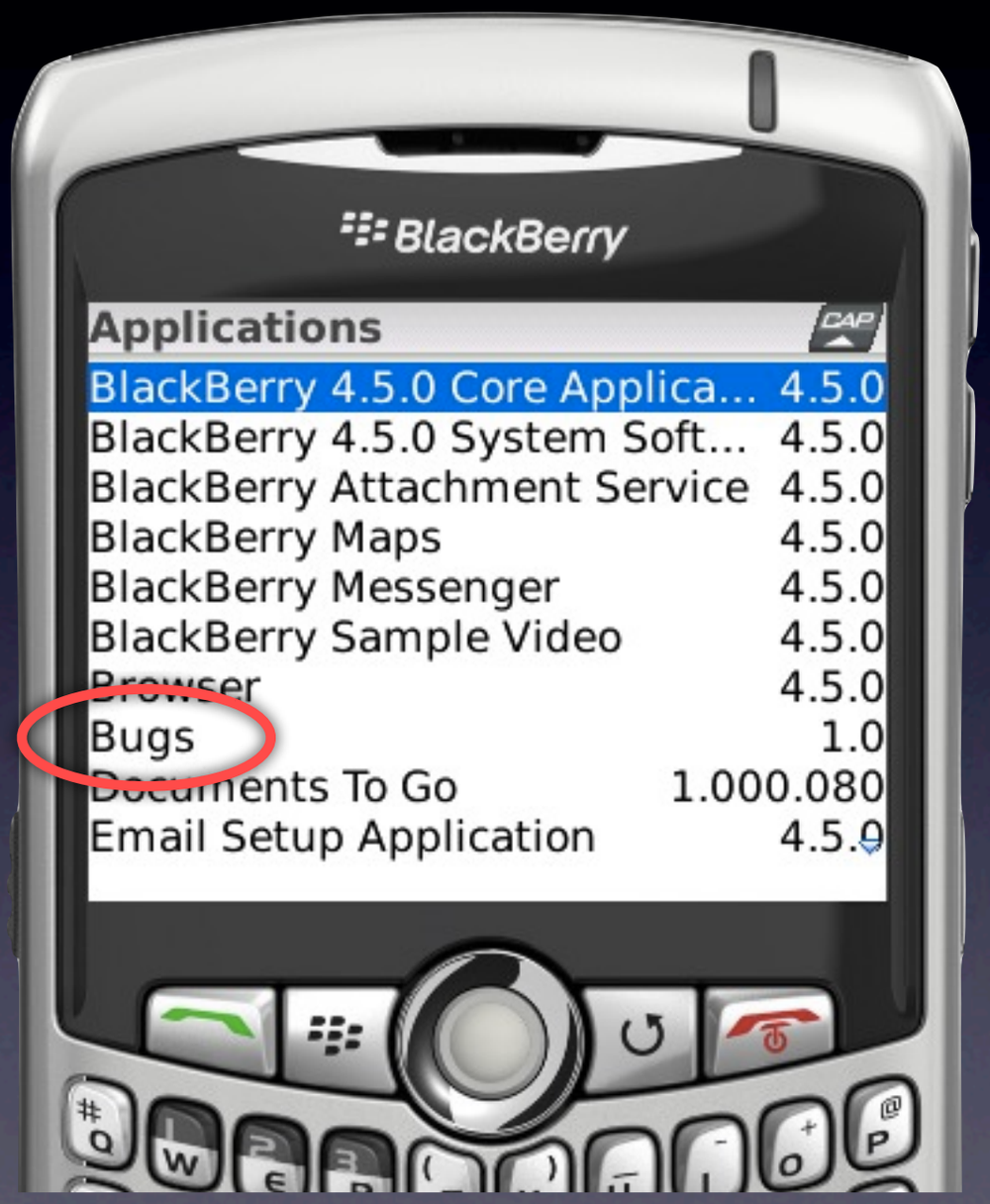
Bugs

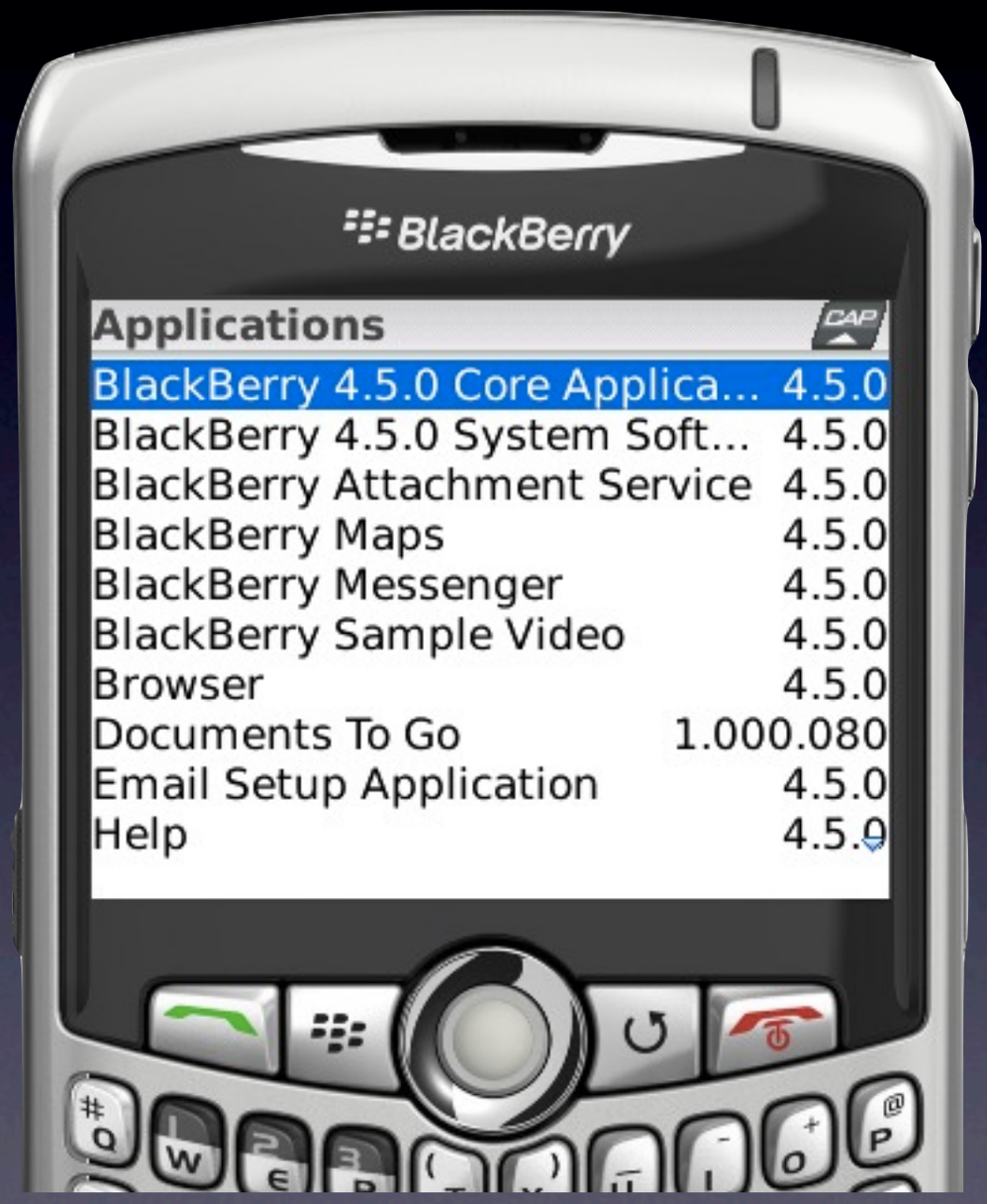

BlackBerry
Applications
BlackBerry 4.5.0 Core Applica... 4.5.0
BlackBerry 4.5.0 System Soft... 4.5.0
BlackBerry Attachment Service 4.5.0
BlackBerry Maps 4.5.0
BlackBerry Messenger 4.5.0
BlackBerry Sample Video 4.5.0
Browser 4.5.0
Bugs 1.0
Documents To Go 1.000.080
Email Setup Application 4.5.0

Bugs


BlackBerry
Applications
BlackBerry 4.5.0 Core Applica... 4.5.0
BlackBerry 4.5.0 System Soft... 4.5.0
BlackBerry Attachment Service 4.5.0
BlackBerry Maps 4.5.0
BlackBerry Messenger 4.5.0
BlackBerry Sample Video 4.5.0
Browser 4.5.0
Bugs 1.0
Documents To Go 1.000.080
Email Setup Application 4.5.0

Bugs


BlackBerry
Applications
BlackBerry 4.5.0 Core Applica... 4.5.0
BlackBerry 4.5.0 System Soft... 4.5.0
BlackBerry Attachment Service 4.5.0
BlackBerry Maps 4.5.0
BlackBerry Messenger 4.5.0
BlackBerry Sample Video 4.5.0
Browser 4.5.0
Bugs 1.0
Documents To Go 1.000.080
Email Setup Application 4.5.0


BlackBerry
Applications
BlackBerry 4.5.0 Core Applica... 4.5.0
BlackBerry 4.5.0 System Soft... 4.5.0
BlackBerry Attachment Service 4.5.0
BlackBerry Maps 4.5.0
BlackBerry Messenger 4.5.0
BlackBerry Sample Video 4.5.0
Browser 4.5.0
Documents To Go 1.000.080
Email Setup Application 4.5.0
Help 4.5.0

Kisses

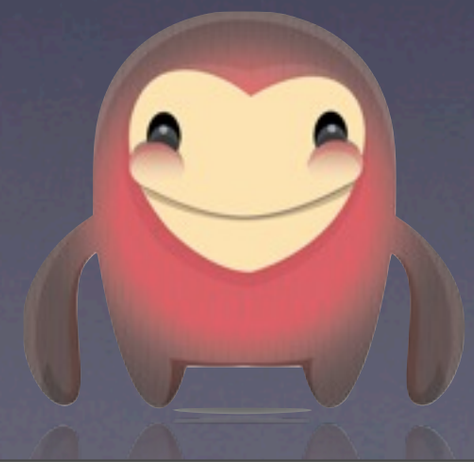
Finds Bugs & other similar, hidden software

Simplifies the search for hidden apps.

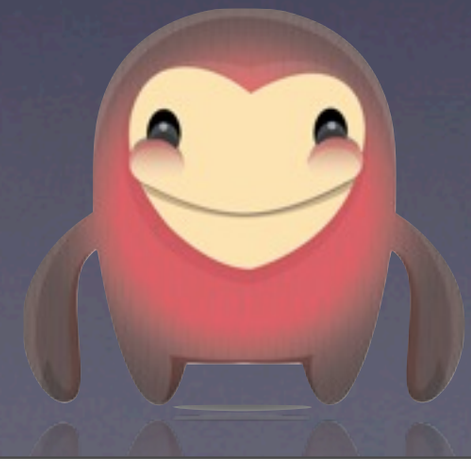
Today: Reveals the presence of Bugs

Download:

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



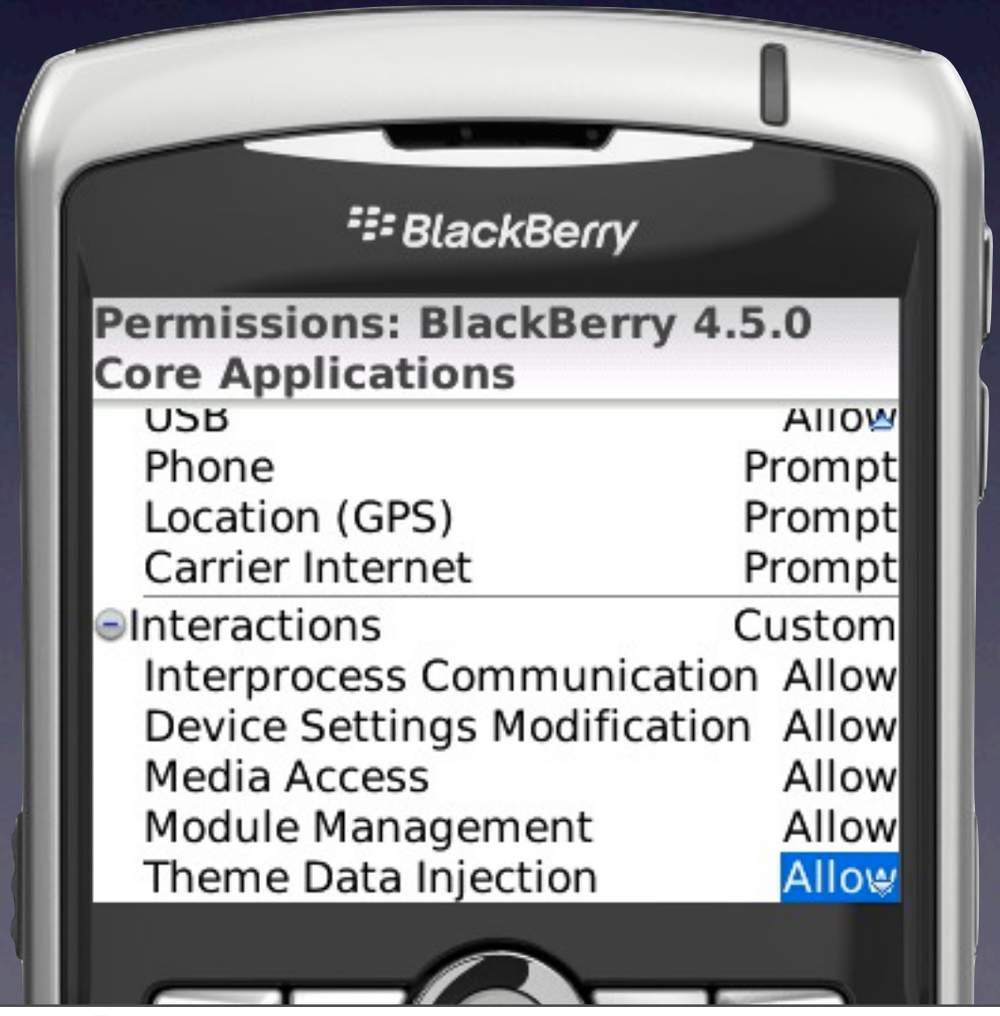
Kisses

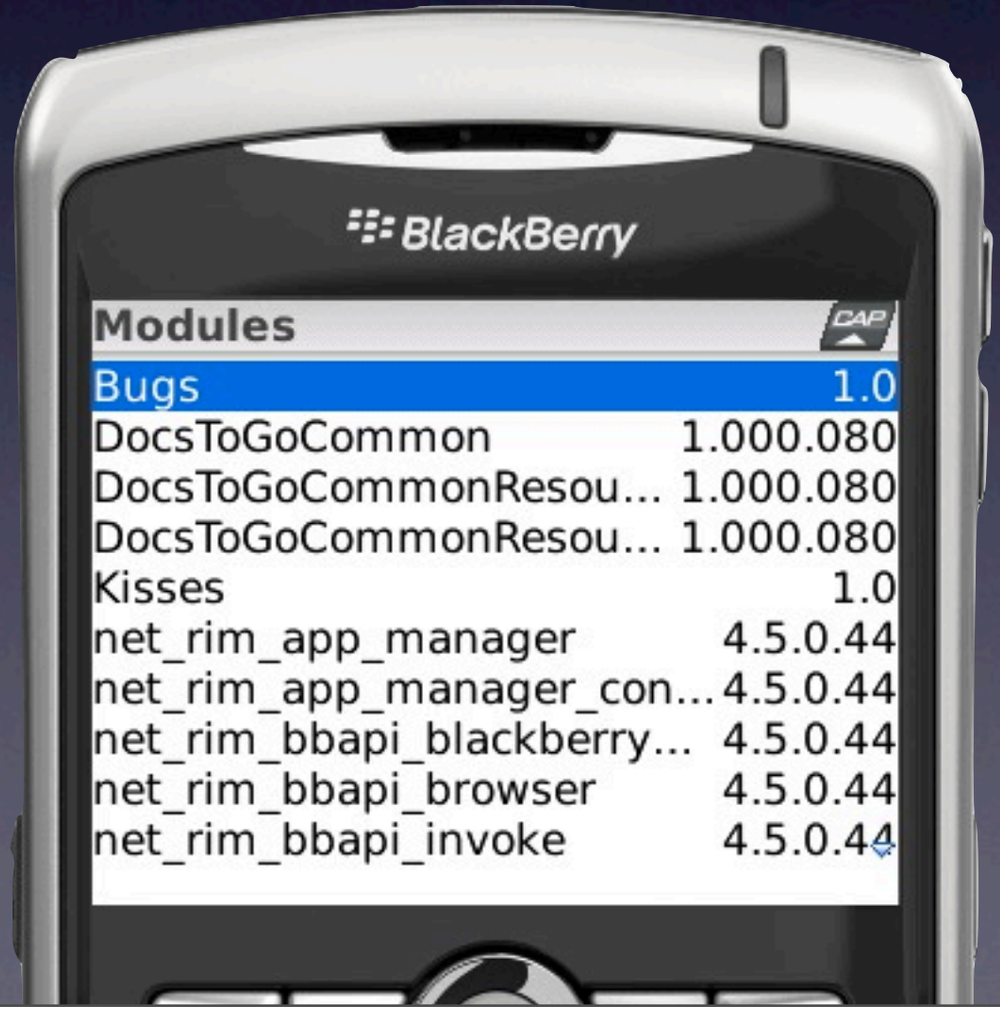


Wrapping up

The BlackBerry is very secure

The problem lies in its complexity





Wrapping up

BlackBerry apps are not regulated

Nothing between you & spyware

iPhone AppStore is good

They check each app.

Watch out

Watch out

Don’t install random pieces of software

Watch out

Don’t install random pieces of software

Limit the amount of software on your BB

Watch out

Don’t install random pieces of software

Limit the amount of software on your BB

Learn and set Default Application Permissions

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

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

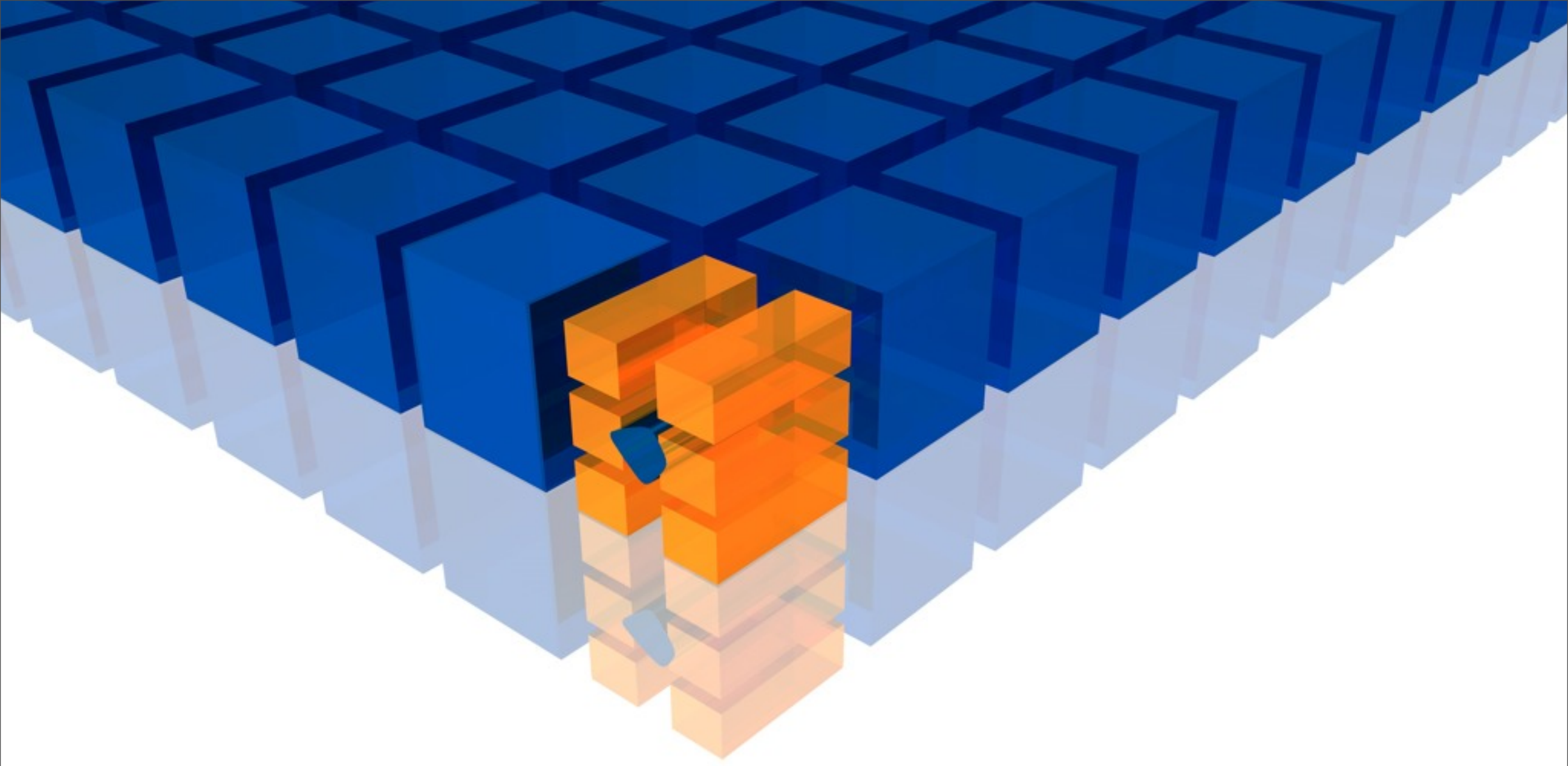
sheran@hermisconsulting.com

sheran@zenconsult.net

http://chirashi.zensay.com

@chopstick_

Questions?



Hermis Consulting

Thank you