Taddong

www.taddong.com

A practical attack against GPRS/EDGE/UMTS/HSPA mobile data communications

David Perez

Jose Pico

Introduction

- It has been proved that GSM is vulnerable to multiple attacks (rogue base station, cryptographic, SMS, OTA, etc.)
- Rogue Base Station attacks have been demonstrated before against GSM, e.g.:
  - PRACTICAL CELLPHONE SPYING. Chris Paget. DEF CON 18 (July 2010) *http://www.defcon.org/html/defcon-18/dc-18-speakers.html*

Introduction

- Is it possible to extend these attacks to GPRS/EDGE, i.e., to mobile data transmissions?

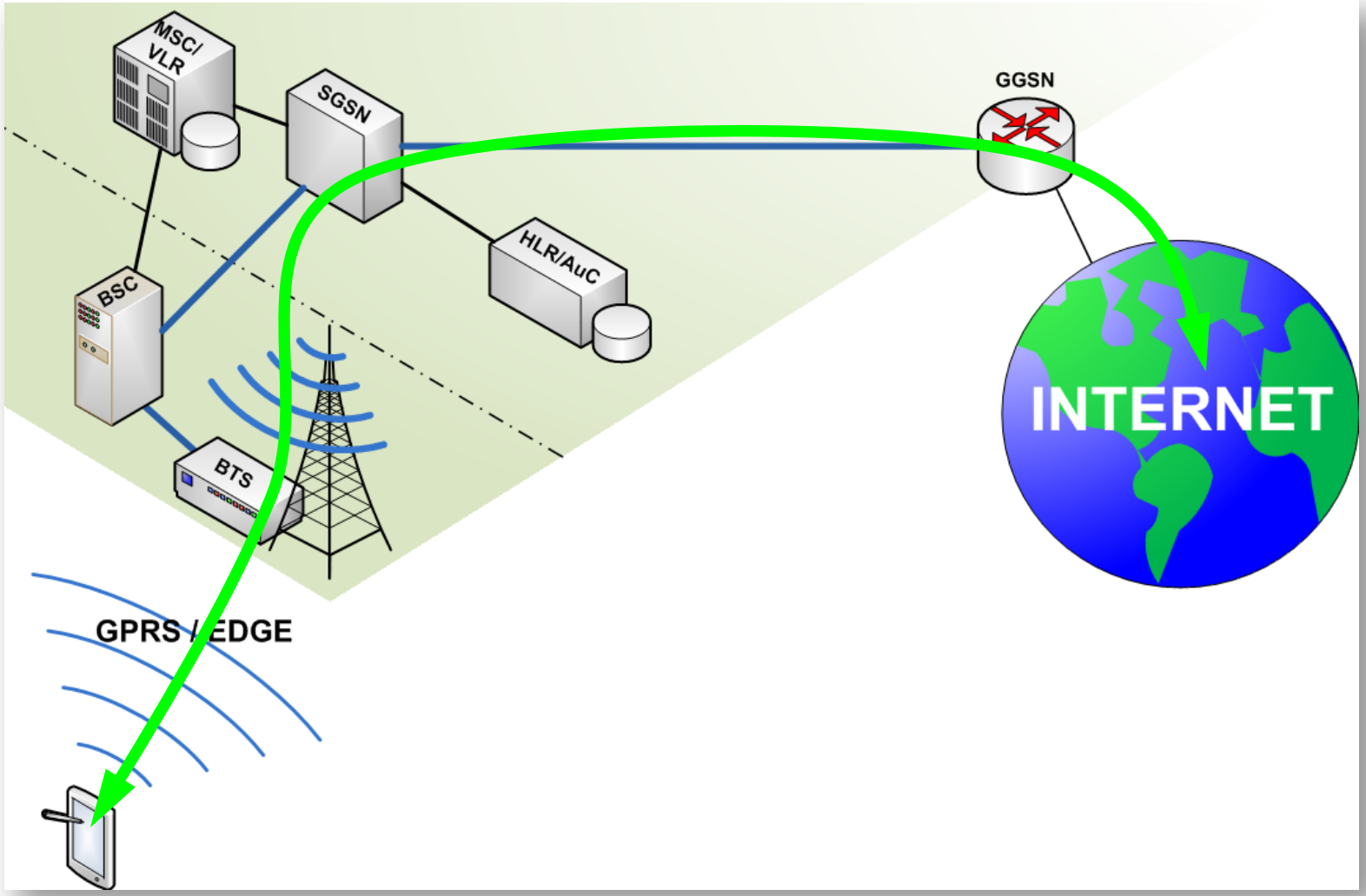
- If YES, what is the impact of such attack?

Introduction

Objectives

- In this presentations we will show that GPRS/EDGE is also vulnerable to rogue base station attacks, just like GSM
- We will describe:
  - The vulnerabilities that make this attack possible
  - The tools that can be used to perform the attack
  - How to perform the attack
  - How to extend this attack to UMTS
  - What an attacker can gain from it

GPRS/EDGE ARQUITECTURE



The vulnerabilities

- Lack of mutual authentication
- GEA0 support
- UMTS→GPRS/EDGE fallback

Just like GSM

The threats

- How many people, organizations, or, in general, entities, might be interested in eavesdropping and/or manipulating the mobile data communications of other entities, like competitors, nation enemies, etc?
- And how many of those potential attacking entities could dedicate a budget of $10,000 to this purpose?

The tools


PoE
Power
Adapter
BTS
HUB/SWITCH
LAPTOP
INTERNET UPLINK
(ADSL/2G/3G)

The tools

A real attacker won't need this, but...

We run all our tests inside a faraday cage, to avoid emissions into the public air interface (Um)

The tools

ip.access nanoBTS

- Commercial BTS
- GSM/GPRS/EDGE capable
- Manufactured by ip.acccess (*www.ipaccess.com*)
- IP-over-Ethernet Abis interface

The tools

PC

- GNU/Linux OS
- Uplink to the Internet
- Small netbook is enough

The tools

OpenBSC

- Awesome work from Harald Welte, Dieter Spaar, Andreas Evesberg and Holger Freyther
- *http://openbsc.osmocom.org/trac/*

> "[OpenBSC] is a project aiming to create a Free Software, GPL-licensed Abis (plus BSC/MSC/HLR) implementation for experimentation and research purpose. What this means: OpenBSC is a GSM network in a box software, implementing the minimal necessary parts to build a small, self-contained GSM network."

The tools

OsmoSGSN

- Included in OpenBSC
- *http://openbsc.osmocom.org/trac/wiki/osmo-sgsn*

> "OsmoSGSN (also spelled osmo-sgsn when referring to the program name) is a Free Software implementation of the GPRS Serving GPRS Support Node (SGSN). As such it implements the GPRS Mobility Management (GMM) and SM (Session Management). The SGSN connects via the Gb-Interface to the BSS (e.g. the ip.access nanoBTS), and it connects via the GTP protocol to a Gateway GPRS Support Node (GGSN) like OpenGGSN"

The tools

OpenGGSN

- Started by: Jens Jakobsen
- Currently maintained by: Harald Welte
- *http://sourceforge.net/projects/ggsn/*

> "OpenGGSN is a Gateway GPRS Support Node (GGSN). It is used by mobile operators as the interface between the Internet and the rest of the mobile network infrastructure."

The tools

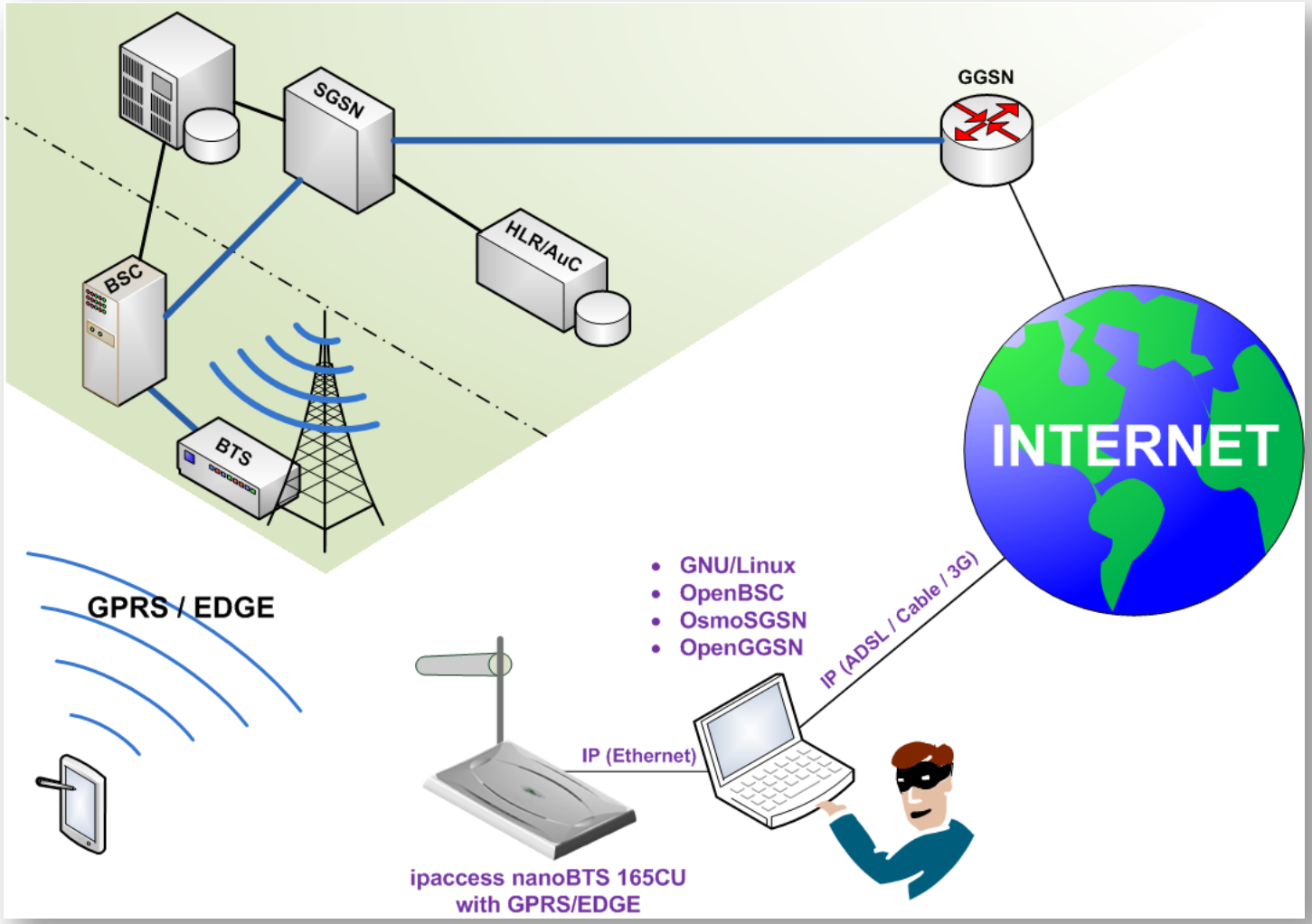
Cell-phone jammer

- Capable of jamming the frequency bands assigned to UMTS/HSPA in a particular location, while leaving the GSM/GPRS/EDGE bands undisturbed

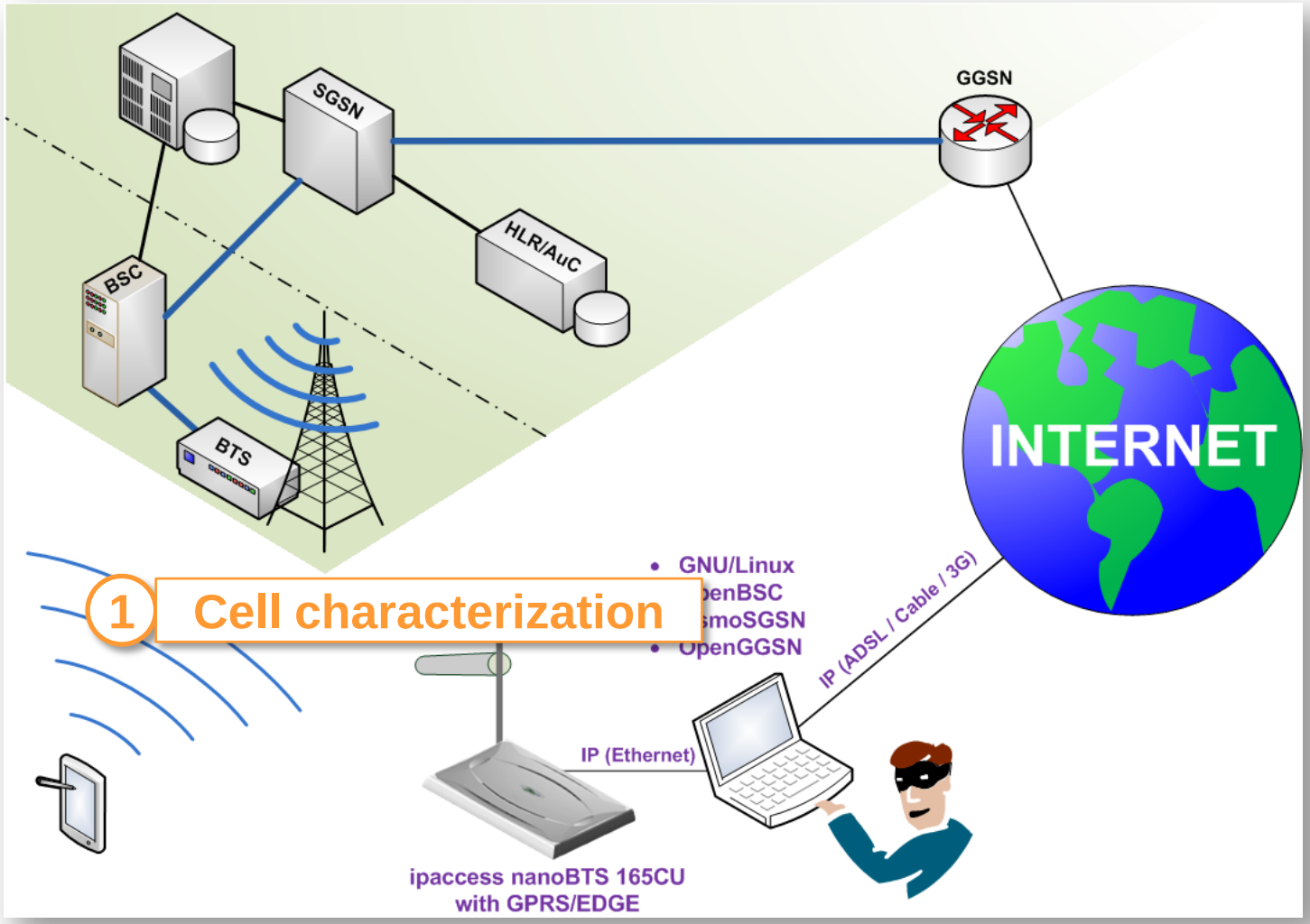
> "A mobile phone jammer is an instrument used to prevent cellular phones from from receiving signals from base stations. When used, the jammer effectively disables cellular phones."
>
> [Source: Wikipedia]

Please note: even *owning* a jammer is illegal in some countries

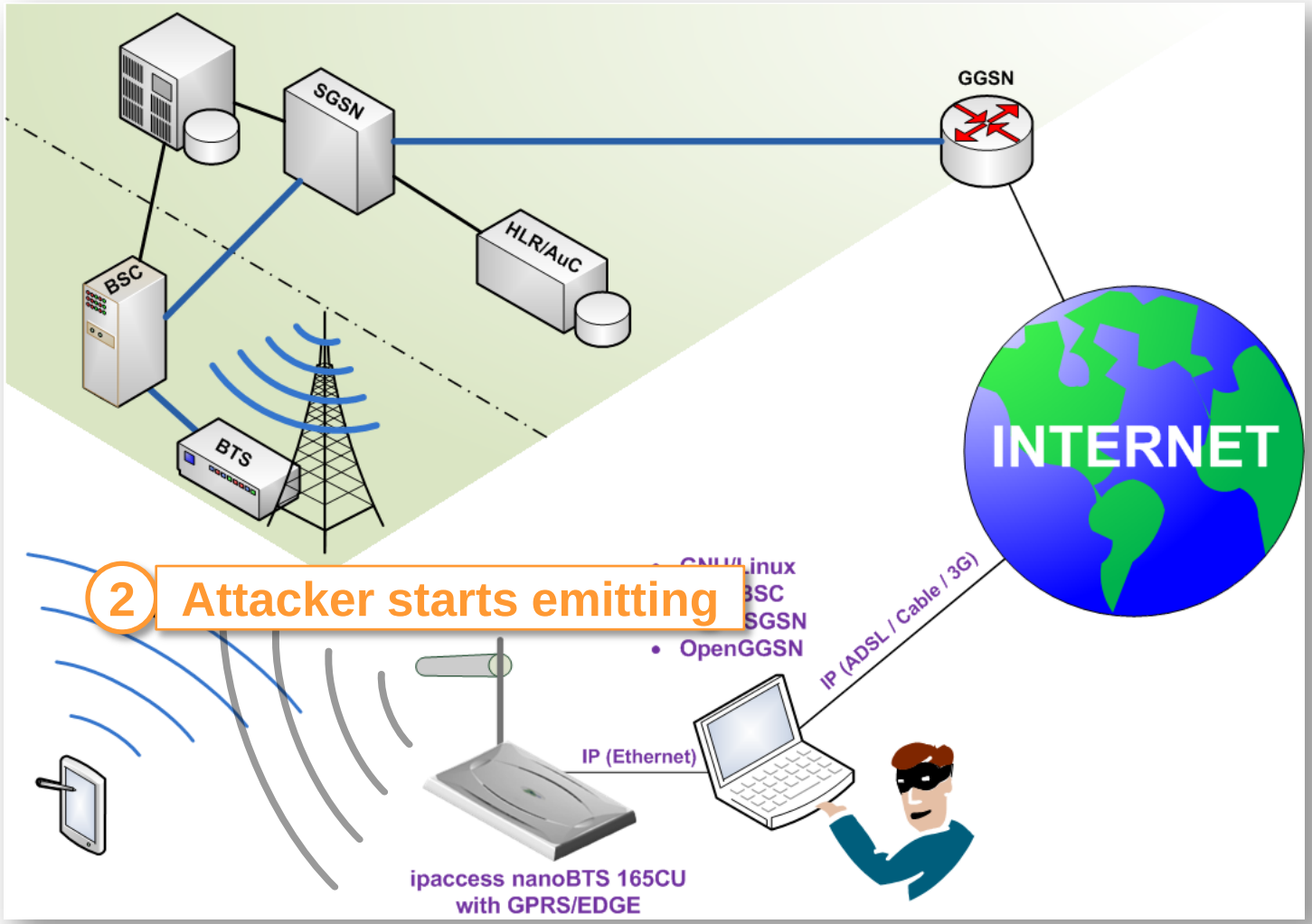
The attack: initial setup



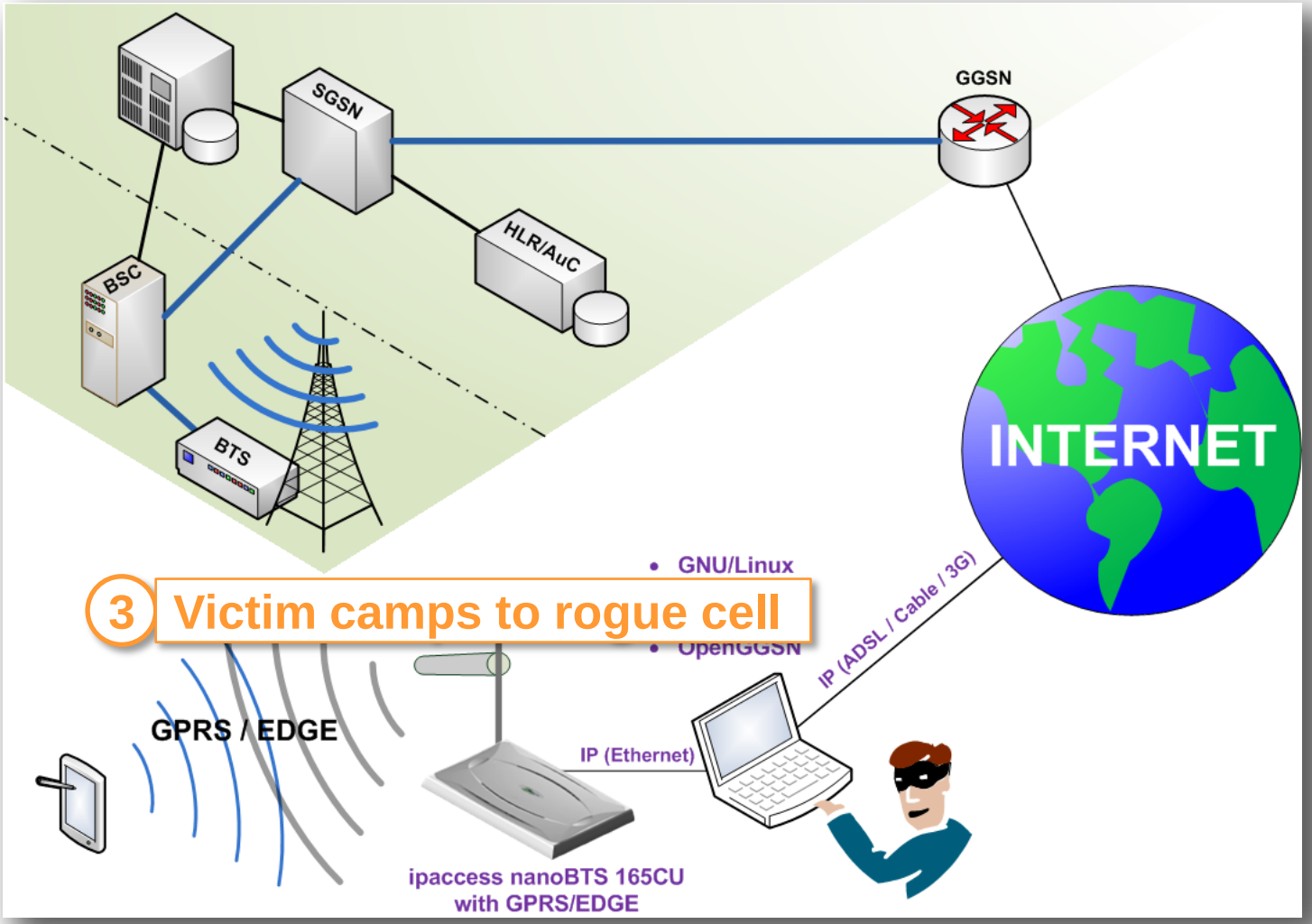
The attack: step 1



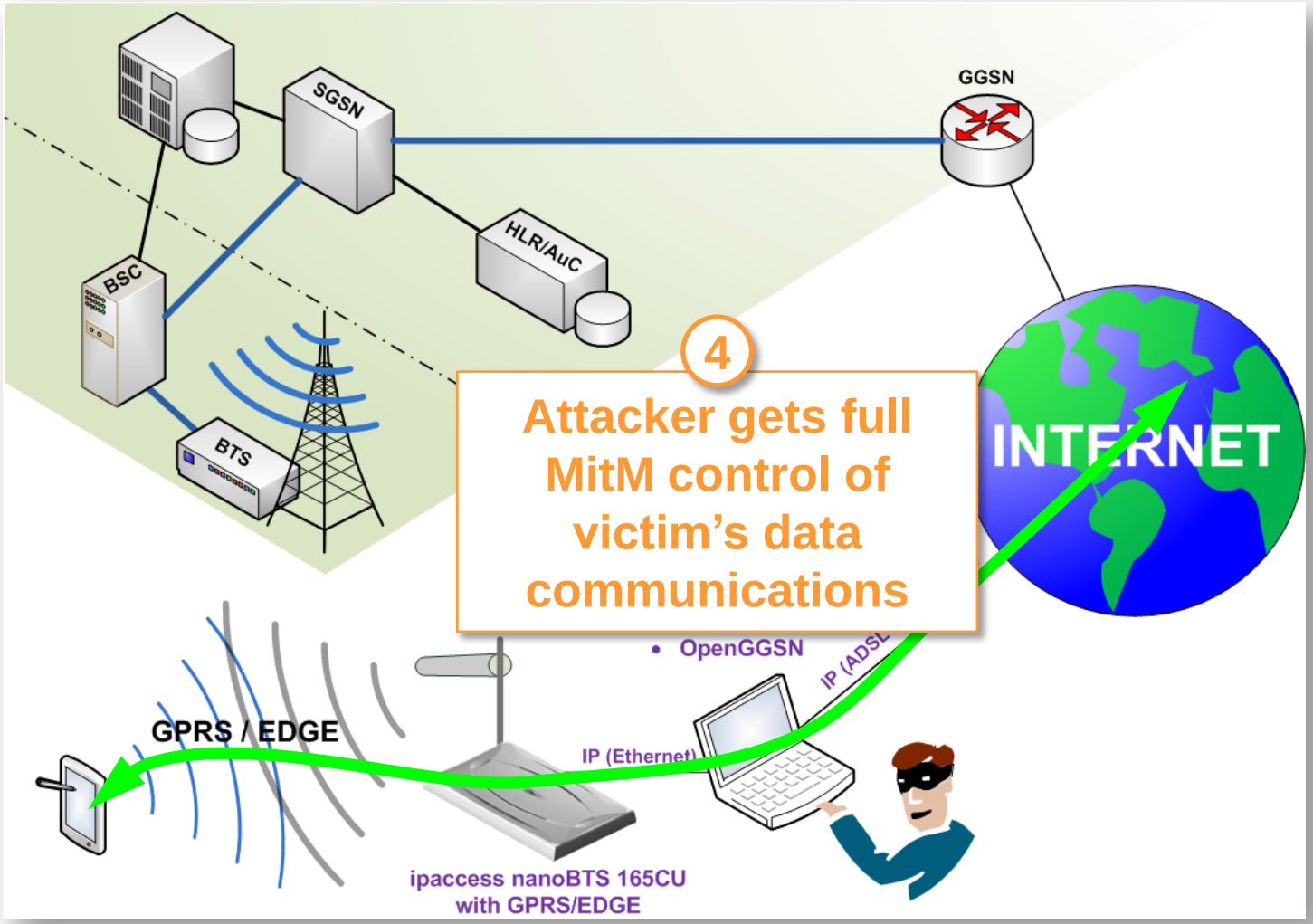
The attack: step 2



The attack: step 3

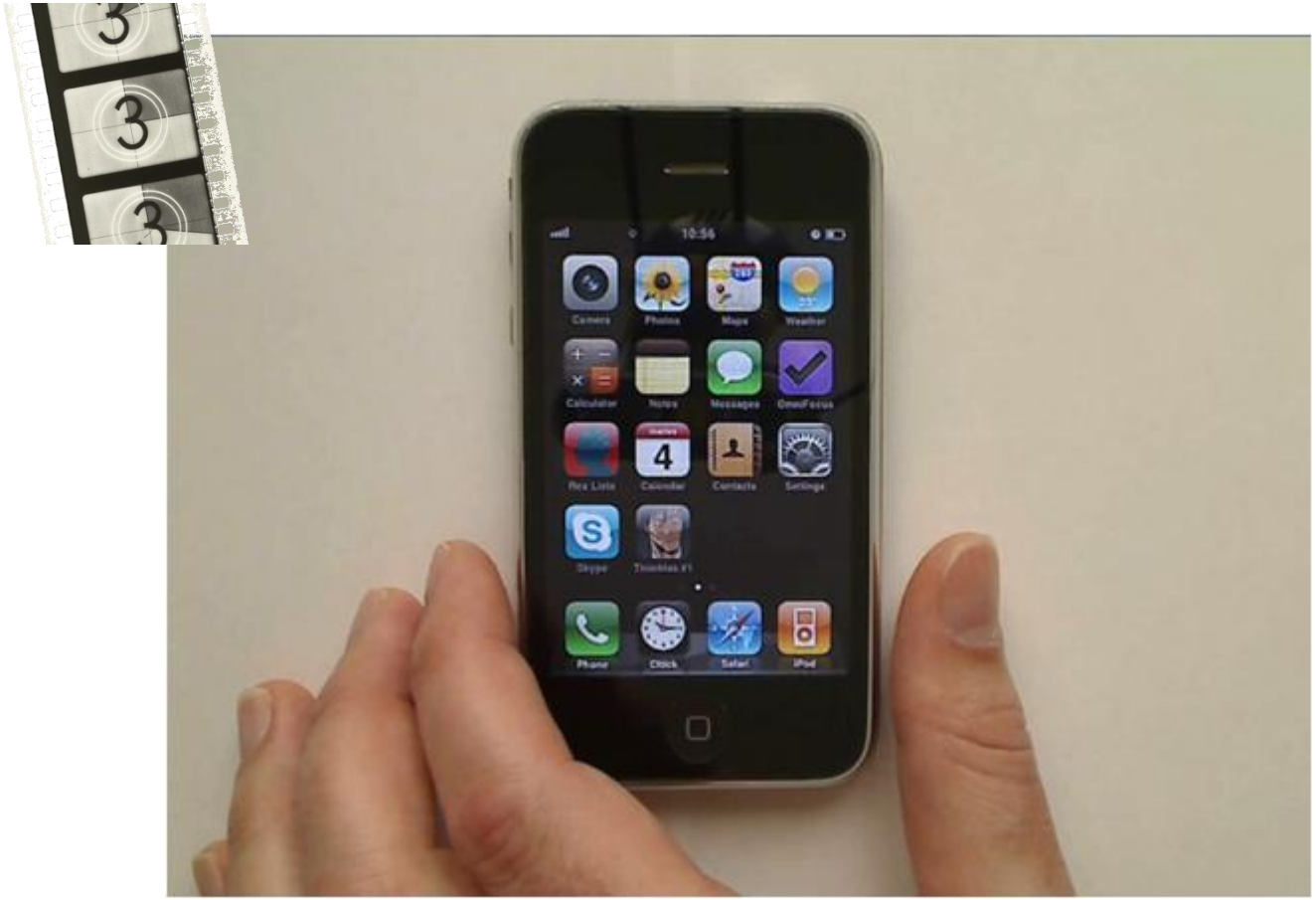


The attack: step 4

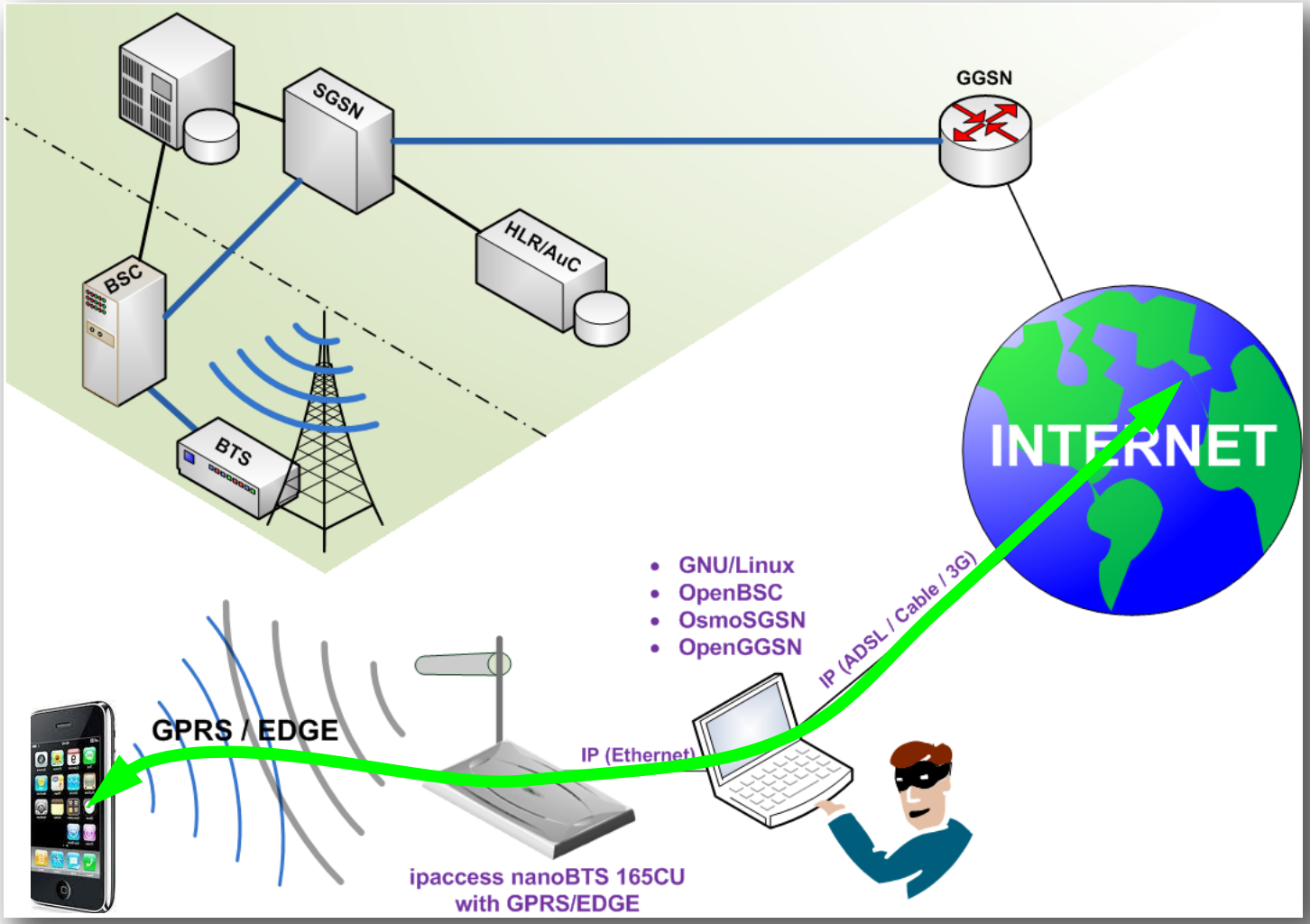


The attack in action

iPhone falls in the rogue base station trap



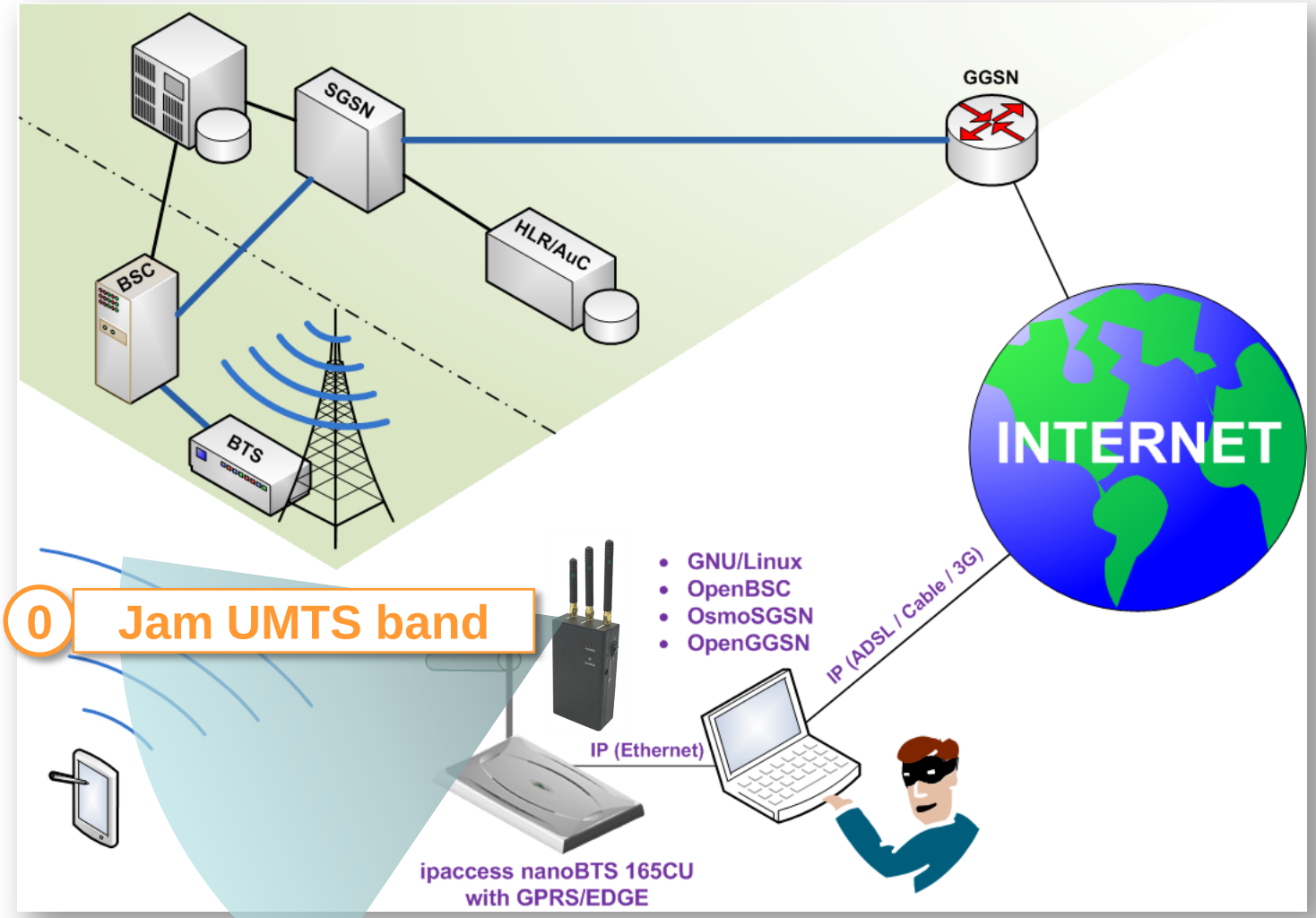
What happened?



Extending the attack to UMTS

How can we extend this attack to UMTS devices?

Extending the attack to UMTS: Simply add step 0

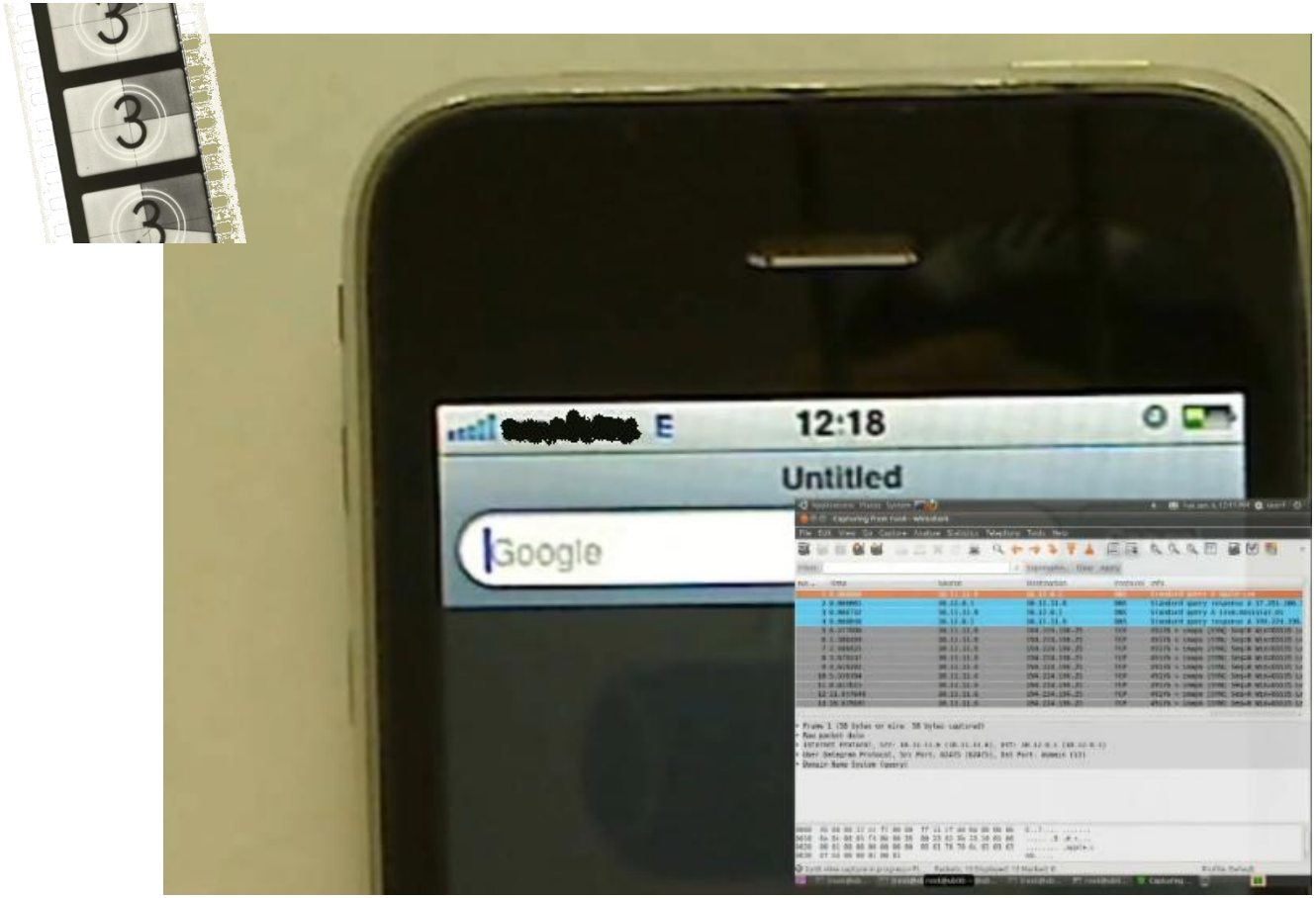


The impact

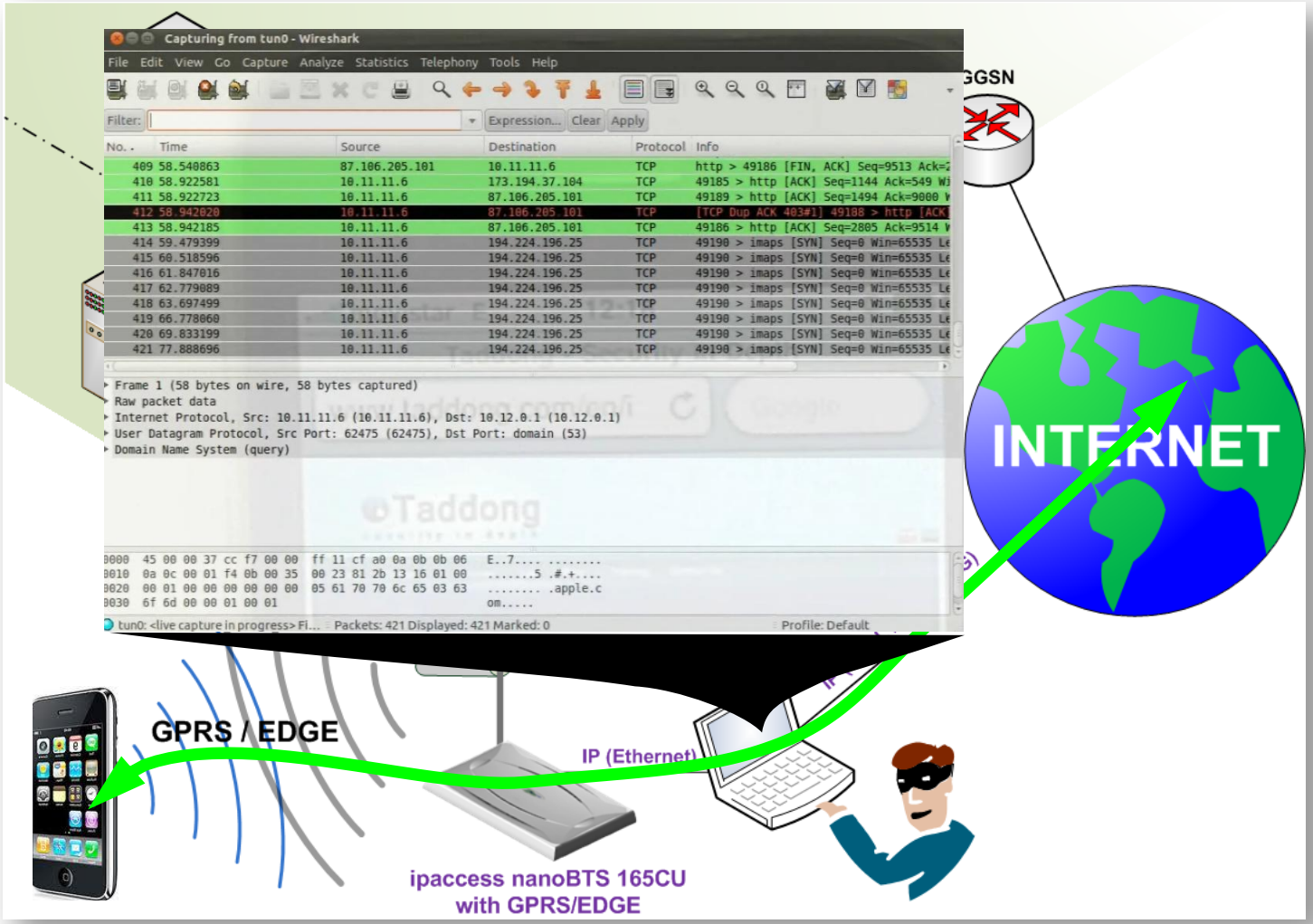
Let us see what an attacker could gain from the attack...

Leveraging the attack: example 1

Attacker sniffs a google search from an iPhone

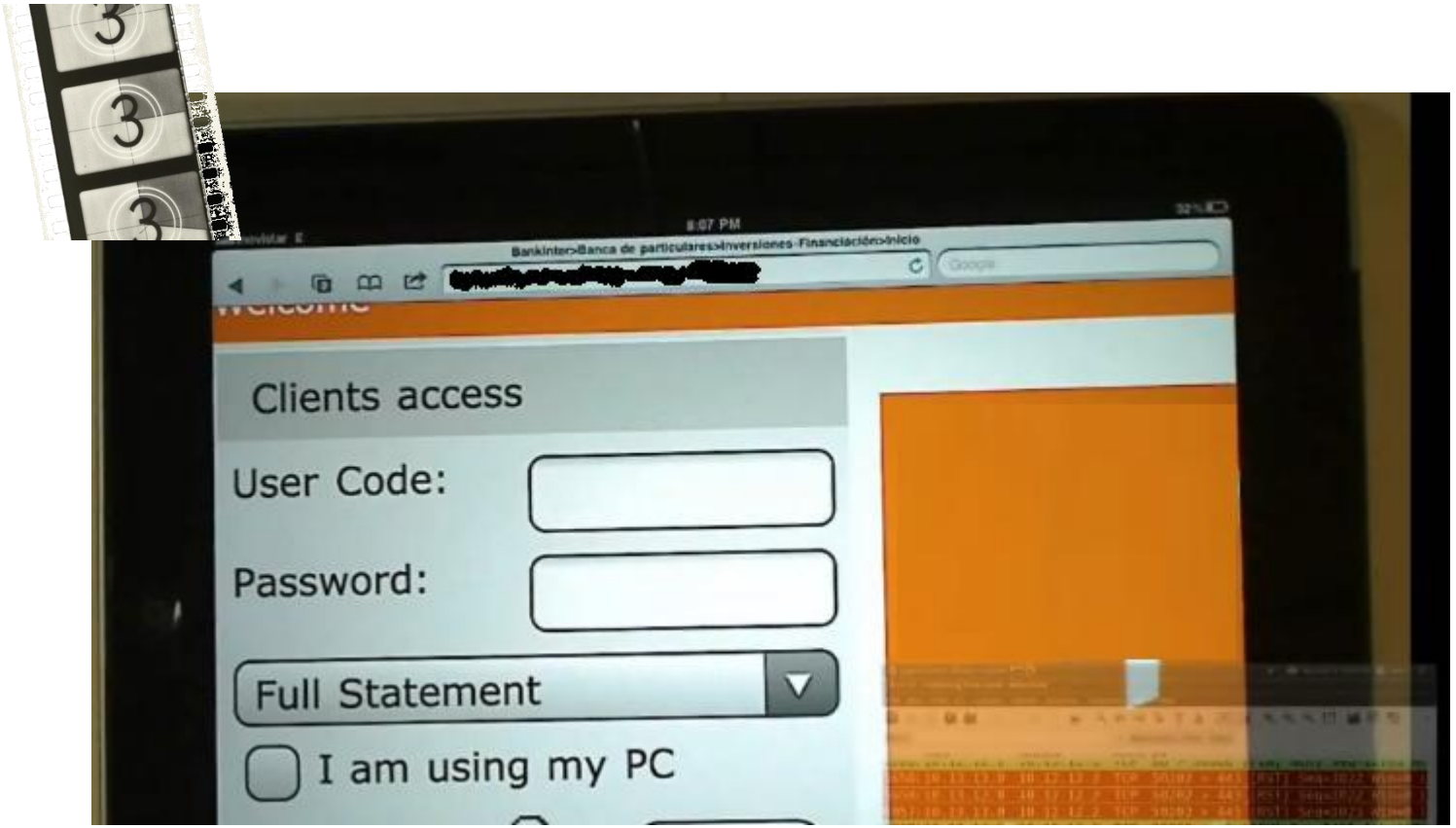


What happened?

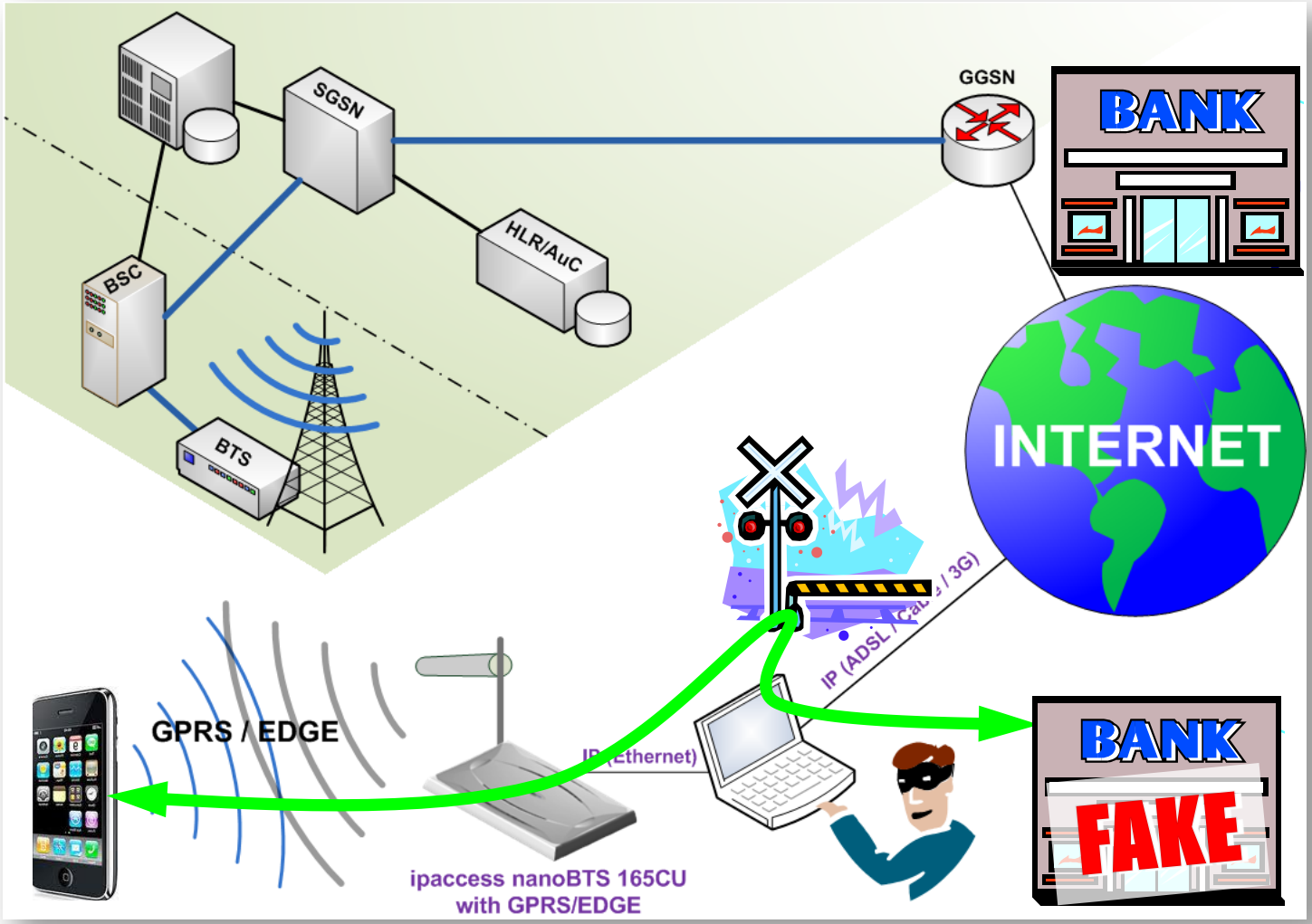


Leveraging the attack: example 2

Phising attack against an iPad (http version)

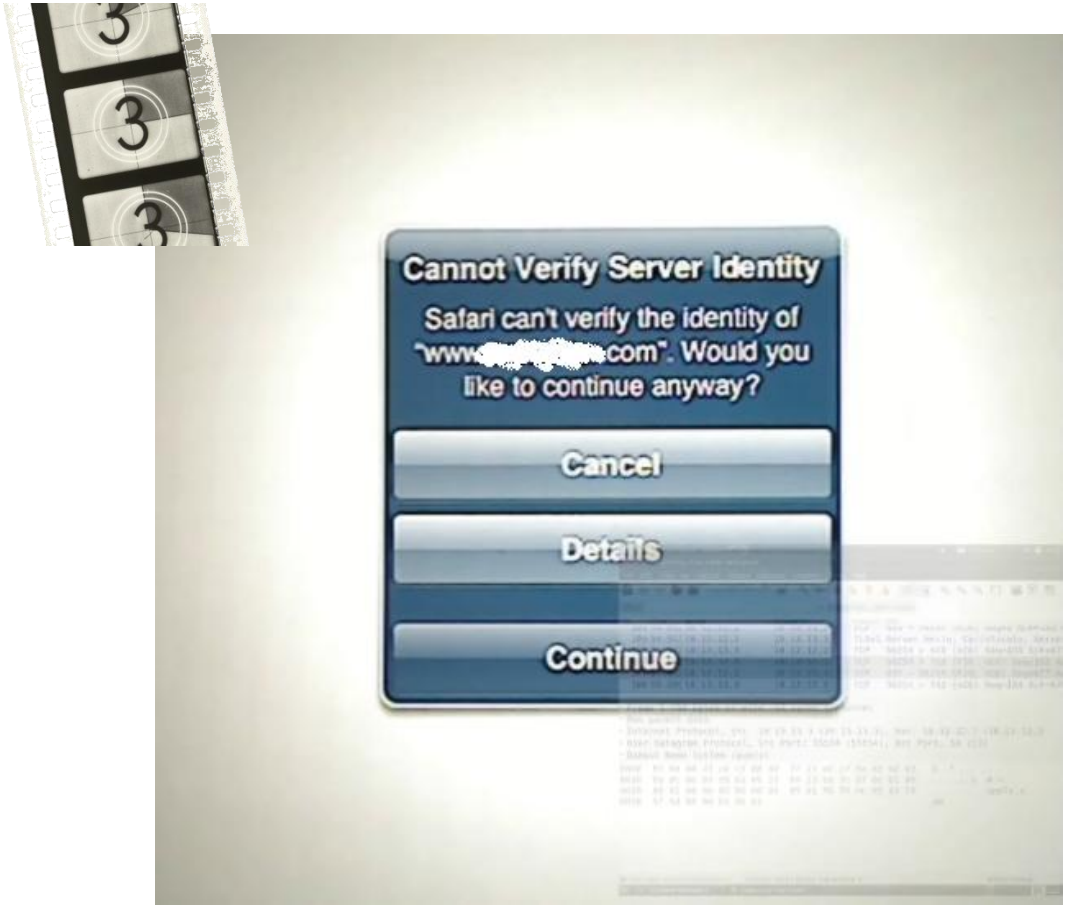


What happened?

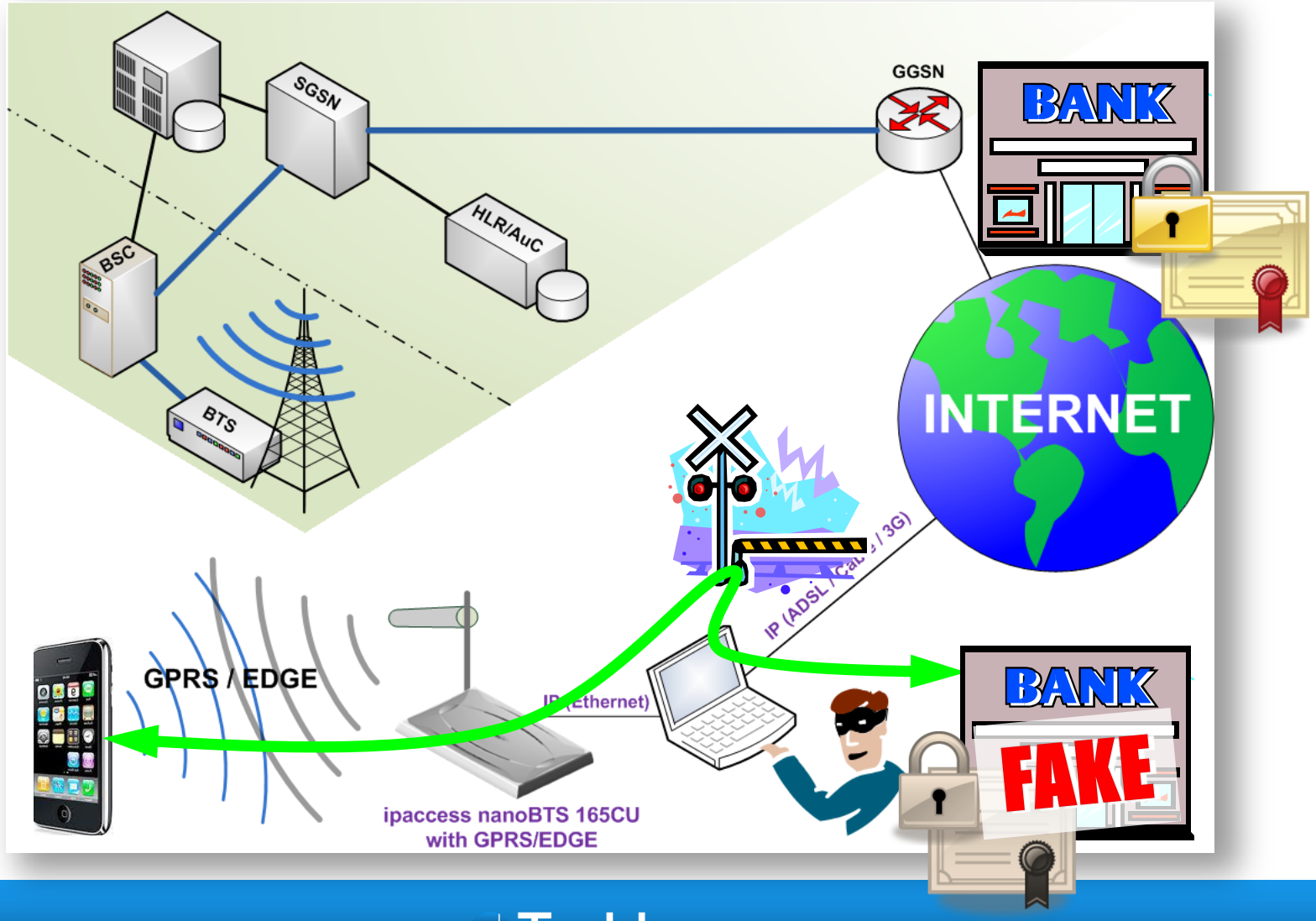


Leveraging the attack: example 3

Phising attack against an iPad (https version)



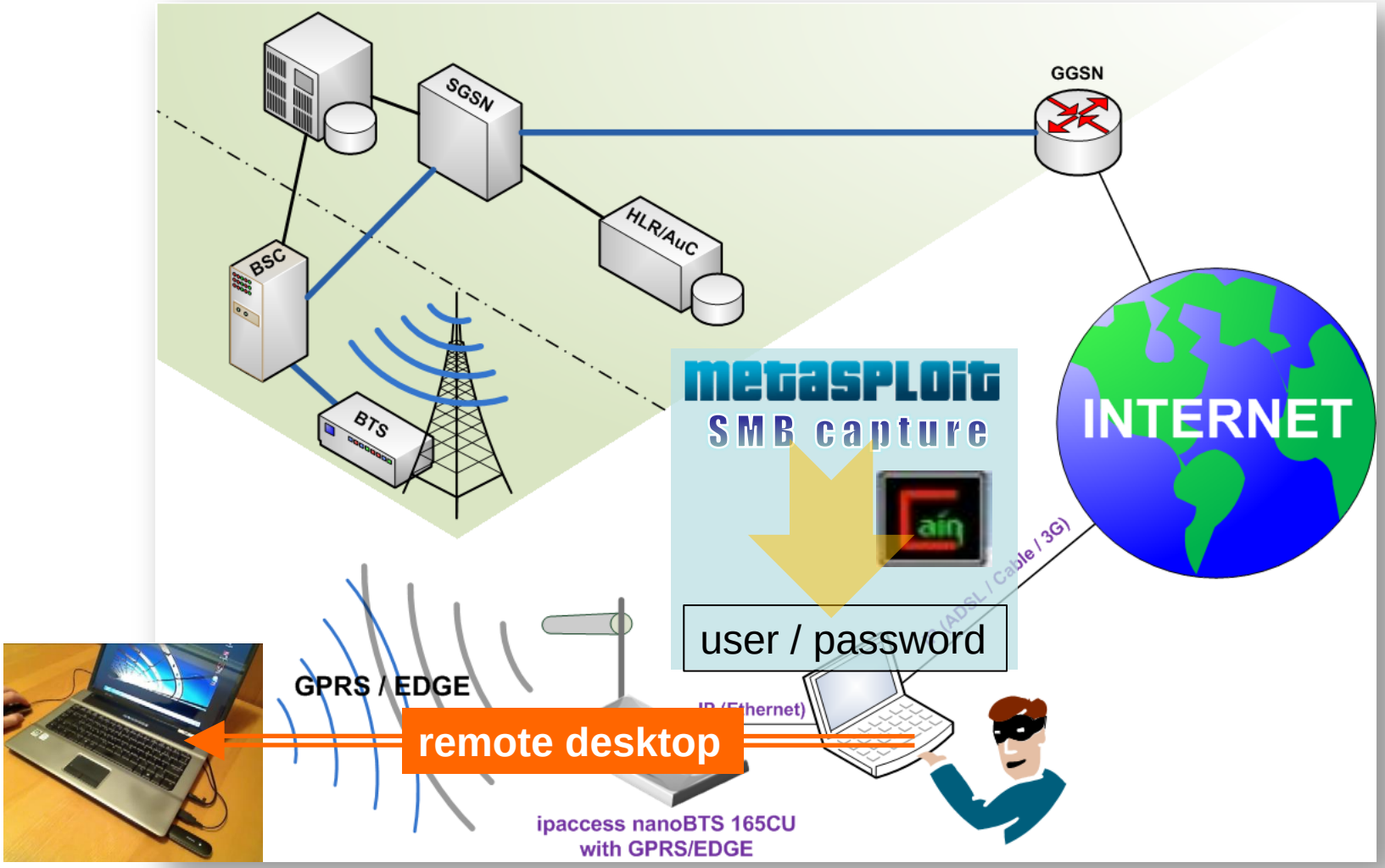
What happened?



Leveraging the attack: example 4

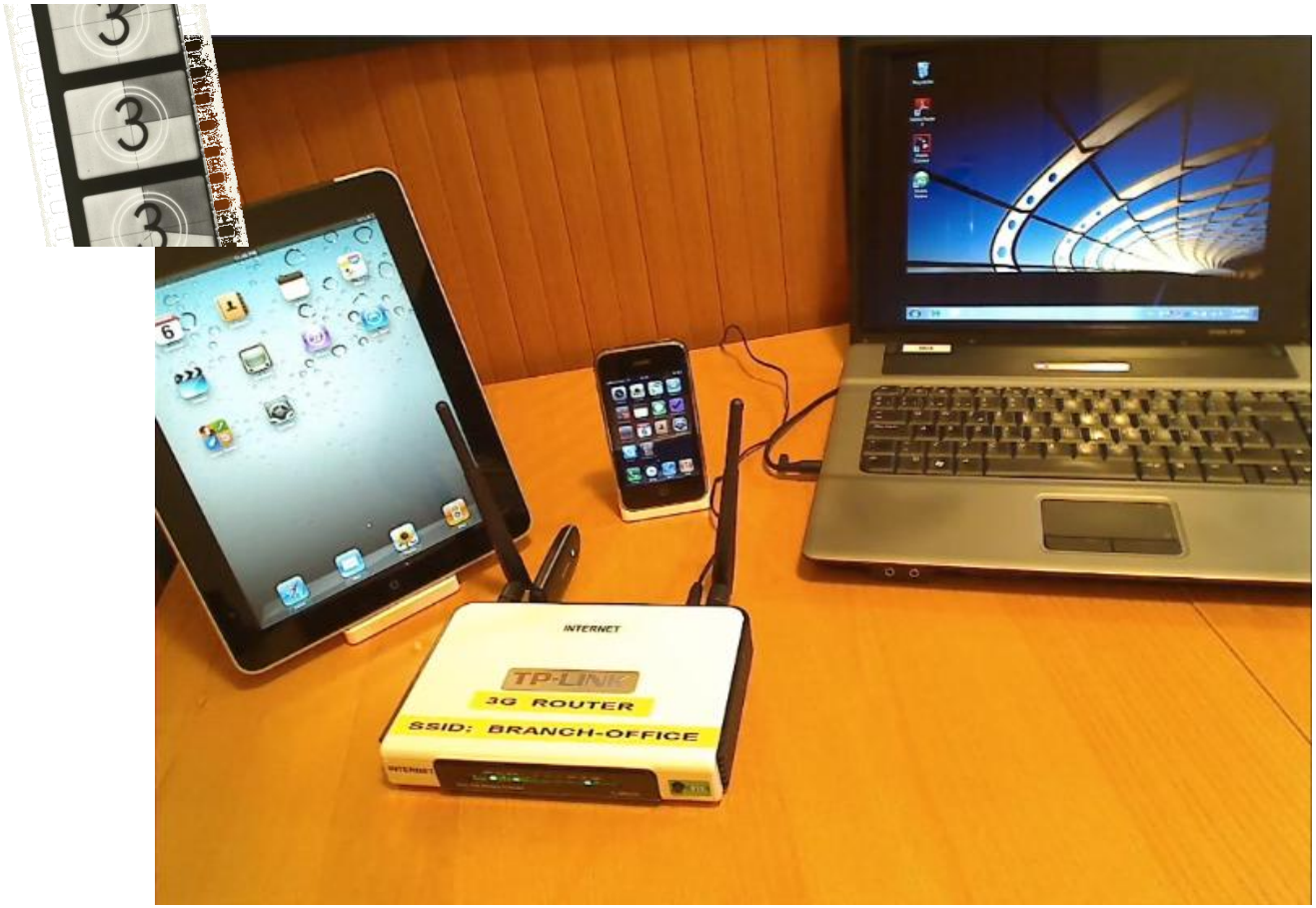
Attacker takes over a Windows PC via GPRS/EDGE

What happened?

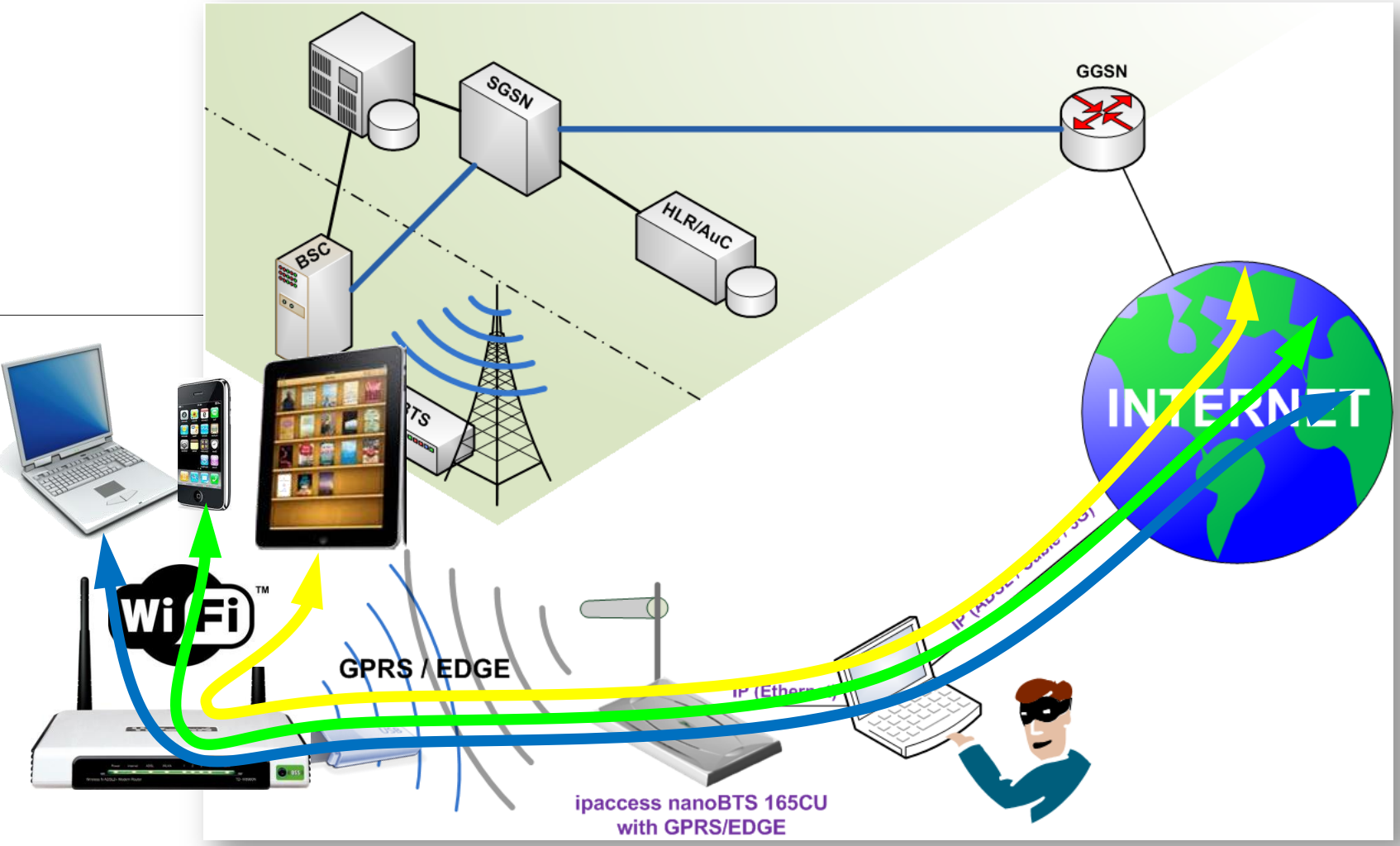


Leveraging the attack: example 5

Attacking a 3G Router in order to control the IP traffic of all devices behind it



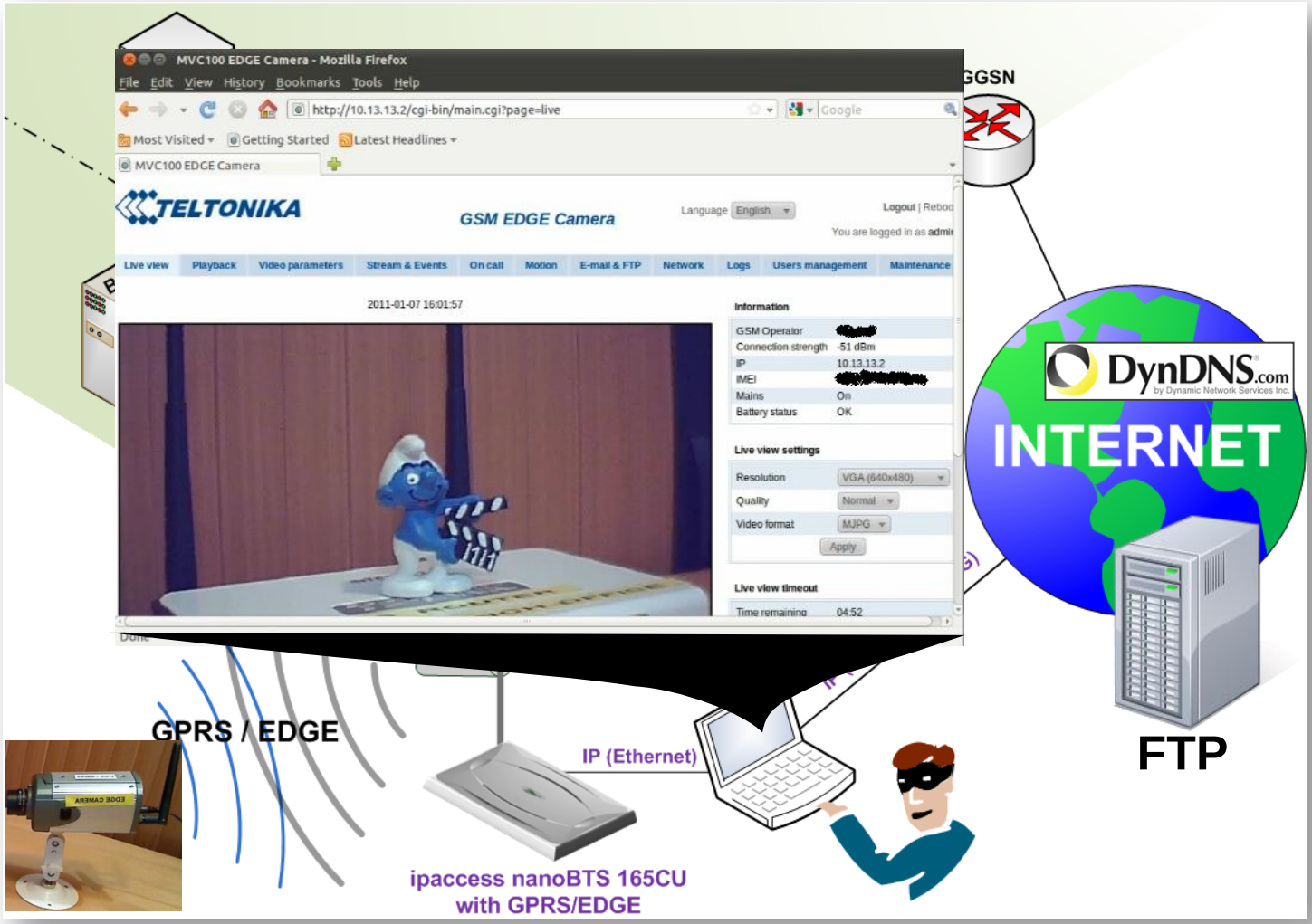
What happened?



Leveraging the attack: example 6

Attacking other GPRS/EDGE devices

What happened?



Defending ourselves

So, what can we do to protect our mobile data communications?

Countermeasures

- Configure our mobile devices to only accept 3G service, rejecting GPRS/EDGE
- Encrypt our data communications at higher layers (https, ssh, IPsec, etc.)
- Install and configure firewall software in our mobile devices

Summing up (I)

A rogue base station attack against GPRS/EDGE devices is totally feasible, just as it is against GSM devices

Summing up (II)

This kind of attack gives an attacker a privileged position to launch IP-based attacks against a GPRS/EDGE device...

...or even to attack the GPRS/EDGE stack itself

Summing up (III)

The attack can be extended to UMTS by simply using a jammer

Effective against any 3G device configured to fall back to GPRS/EDGE when UMTS is not available

Conclusion

We must protect our GPRS/EDGE mobile data communications:

- Know the vulnerabilities
- Evaluate the risks
- Take appropriate countermeasures

Thank you!

David Perez

david@taddong.com

Jose Pico

jose@taddong.com