

Acceso móvil a la nube: un punto vulnerable

David Pérez

José Picó

IX Foro de Seguridad - RedIRIS

Valencia, 10 de Marzo de 2011

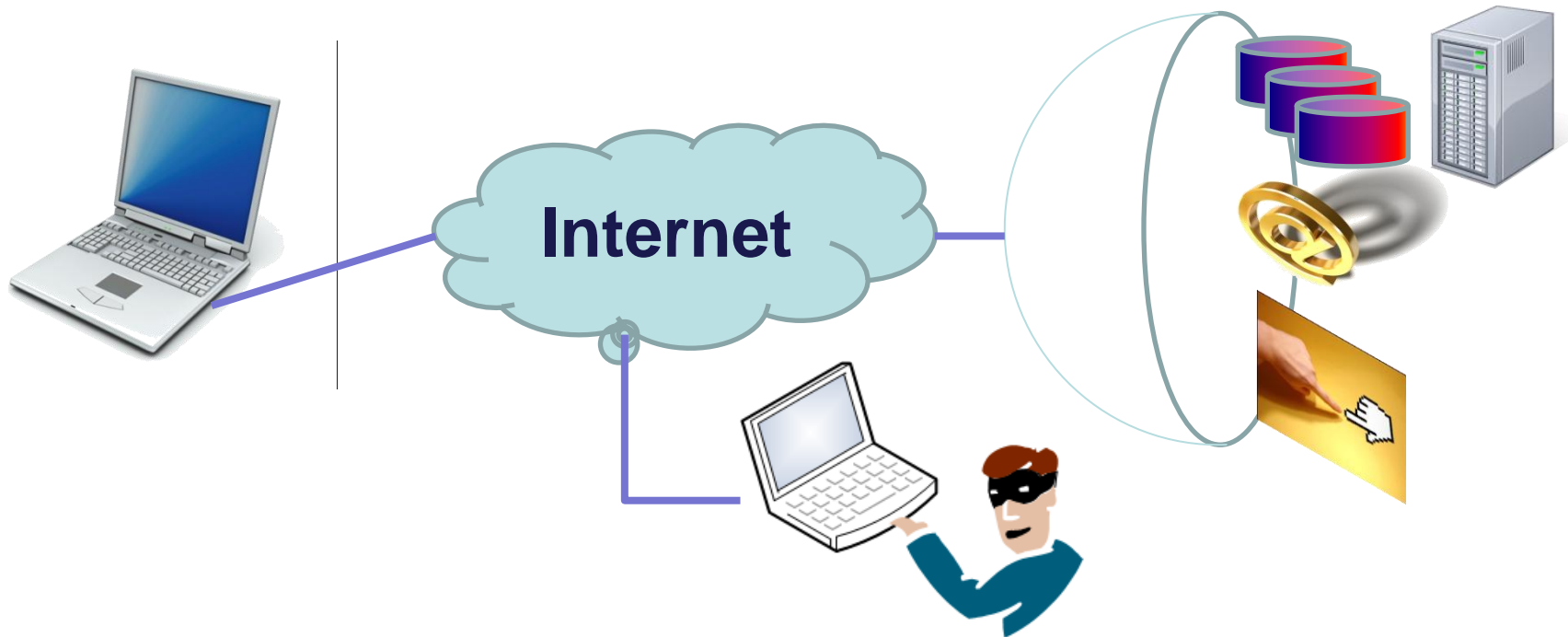
Contenido

- Riesgos en el acceso móvil a la nube
- Posibles ataques a comunicaciones móviles de datos
- El ataque mediante estación base falsa. Implicaciones.
- Ejemplos de ataque
- Medidas de protección

The slide features a white background with decorative blue and black elements. A thick black horizontal line is positioned above the title, and another thick black horizontal line is positioned below it. The blue elements are curved shapes in the top-left and bottom-right corners, and a solid blue bar at the bottom of the slide.

Riesgos en los accesos móviles a la nube

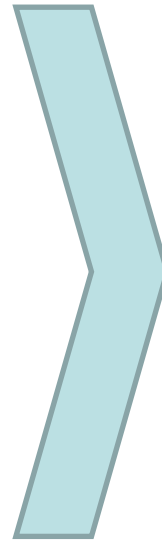
Riesgos en el acceso a los servicios en la nube



- Sistema Operativo y Aplicaciones potencialmente vulnerables
- Comunicaciones a través de Internet
- Acceso a datos internos sensibles

Acceso móvil a internet

- De media, el 68% de los habitantes son usuarios de dispositivos móviles. Este dato continúa creciendo.
- La tasa de usuarios de internet aumentó un 4% en el último año, pero la tasa de líneas de telefonía fija por 100 habitantes descendió hasta el 17,9% en 2009



El uso de Internet
es cada vez más
móvil

(*) Datos extraídos del informe SIE[10
de la Fundación Telefónica

Dispositivos móviles como fuente de amenaza en los accesos a servicios en la nube

- Los accesos a la nube se realizarán, cada vez más, a través de dispositivos móviles
- Son ya una de las vías de ataque en proceso de investigación

Dispositivos móviles como fuente de amenaza en los accesos a servicios en la nube

- Teléfono móvil = ordenador portátil:
 - sistema operativo
 - aplicaciones
 - conexión a Internet (vía Wifi ó 3G)
 - acceso a aplicaciones críticas

Dispositivos móviles como fuente de amenaza en los accesos a servicios en la nube

- Riesgos adicionales de un móvil:
 - Otras conexiones normalmente habilitadas (WiFi, bluetooth)
 - No suele disponer de software de cifrado, VPN, firewall, etc.
 - **2G/3G: canal adicional de comunicaciones, normalmente no contemplado en las acciones preventivas de la seguridad de las organizaciones**
 - En ocasiones, se le asigna una IP pública

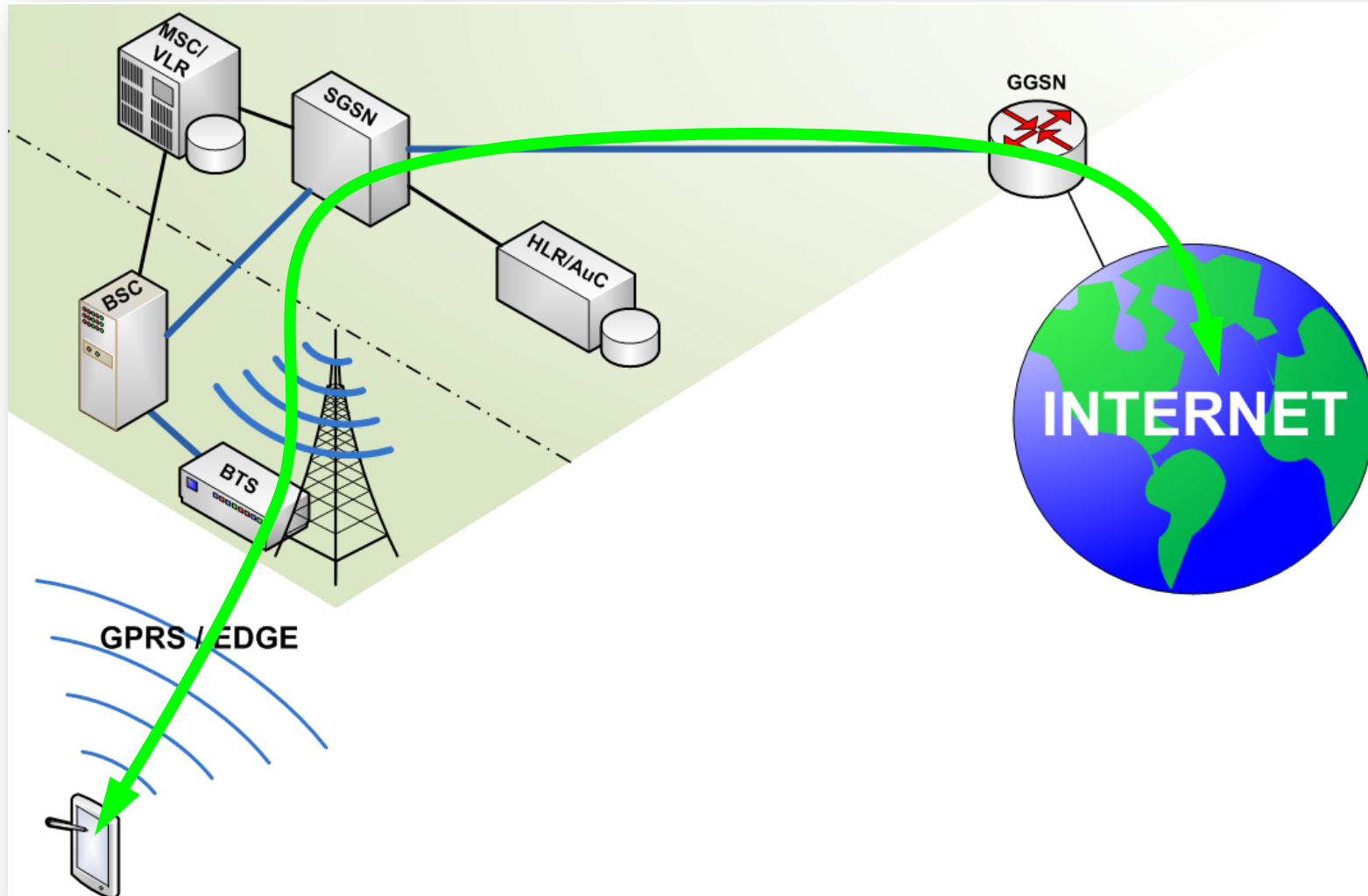
¿Amenaza?

- ¿Existen entidades (personas, organizaciones, gobiernos) interesadas en obtener y/o manipular las conexiones móviles de voz y datos de otras entidades?
- ¿Con 10.000€ de presupuesto?

The slide features a white background with decorative blue and black elements. A thick black horizontal line is positioned above the title, and another thick black horizontal line is positioned below it. The blue elements are curved shapes in the top-left and bottom-right corners.

Posibles ataques a comunicaciones móviles de datos

Arquitectura GPRS/EDGE



Comunicaciones móviles expuestas a varios vectores de ataque



Vulnerabilidades del protocolo



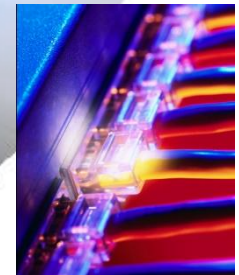
Ataques criptográficos



Ataques OTA



Corrupción de memoria



Desde el operador

Ataque con estación base falsa

Vulnerabilidades

- Autenticación unidireccional
- Soporte a GEA0 (no cifrado)
- Soporte a degradación
UMTS→GPRS/EDGE

Igual que en GSM

Herramientas



Las herramientas

Un atacante no necesitará esto, pero...

Nosotros realizamos todas nuestras pruebas en una caja de Faraday, para evitar emisiones en el espacio público radioeléctrico (Um)



Las herramientas



ip.access nanoBTS



- BTS comercial
- Soporta GSM/GPRS/EDGE
- Fabricada by ip.access (www.ipaccess.com)
- Intefaz IP-over-Ethernet
Abis



Las herramientas

PC



- S.O. GNU/Linux
- Acceso a Internet
- Un pequeño netbook es suficiente

Las herramientas

OpenBSC

- Código desarrollado por Harald Welte, Dieter Spaar, Andreas Evesberg y 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.”

Las herramientas

OsmoSGSN

- Código incluido en 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”

Las herramientas

OpenGGSN

- Código iniciado por: Jens Jakobsen
- Actualmente mantenido por: 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.”



Las herramientas

Inhibidor de frecuencias de móvil (*jammer*)



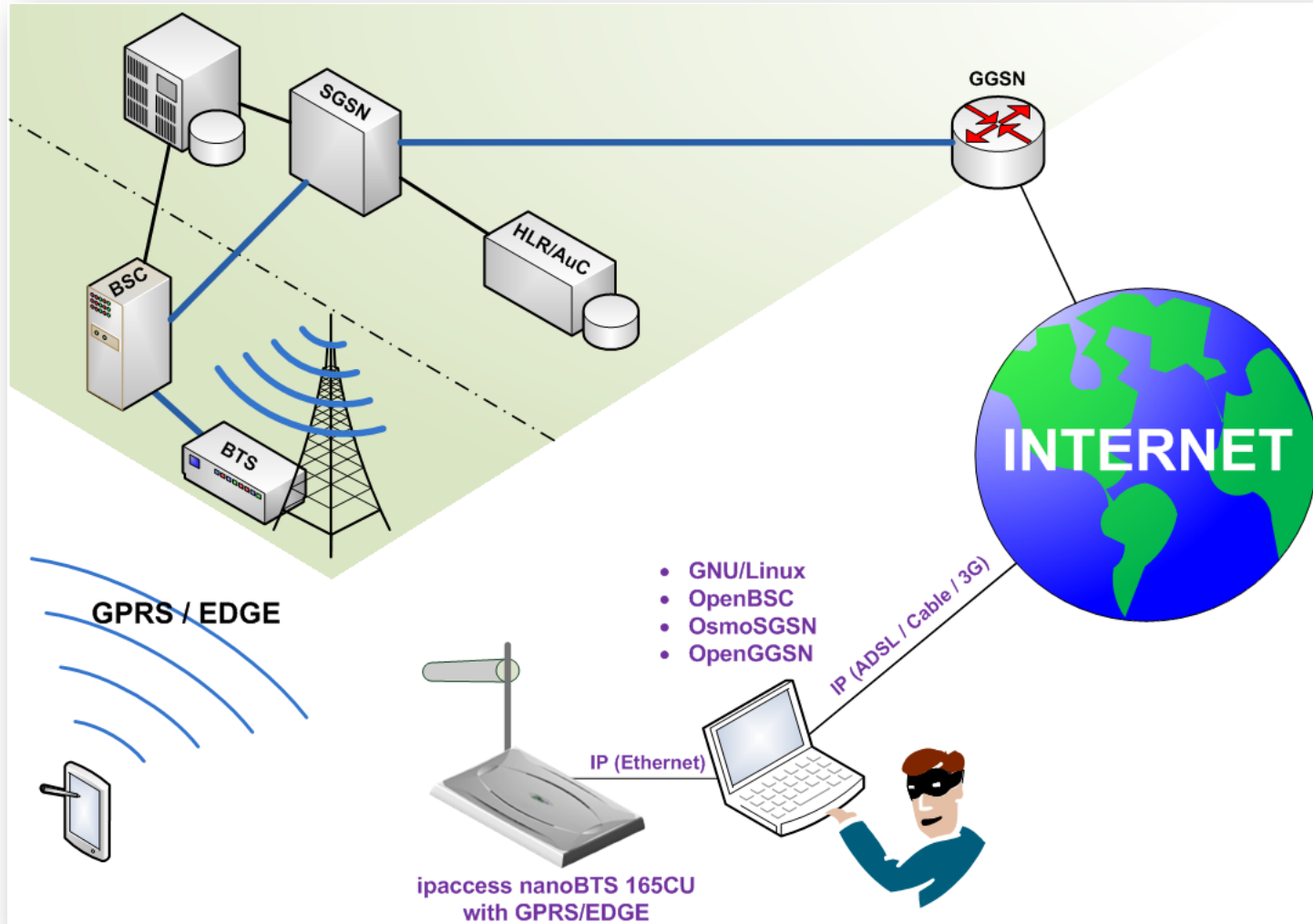
- Capaz de inhibir las frecuencias asignadas a UMTS/HSPA en un lugar determinado, sin perturbar las frecuencias de GSM/GPRS/EDGE

“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.”

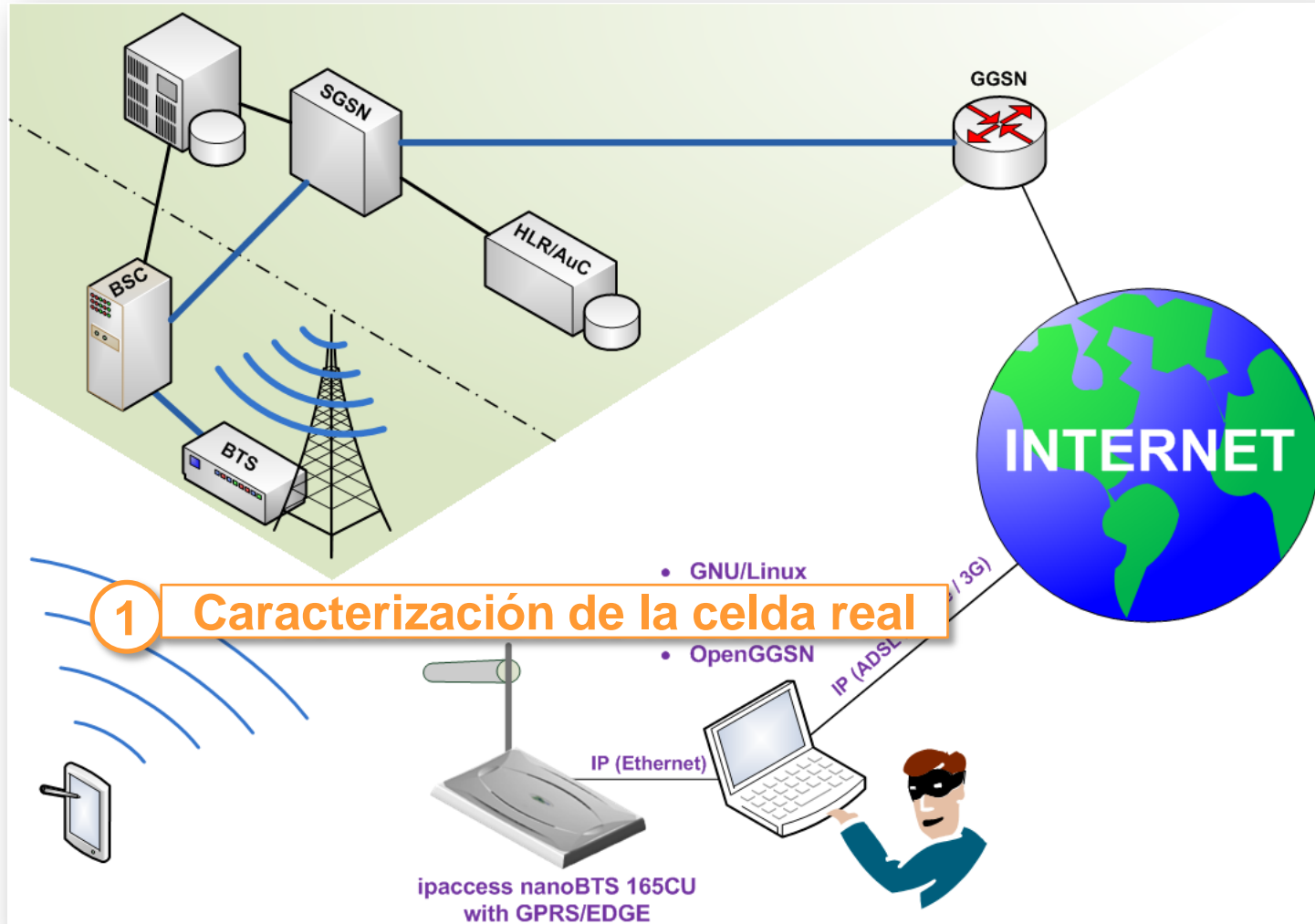
[Source: Wikipedia]

AVISO: Incluso poseer un *jammer* es ilegal en muchos sitios

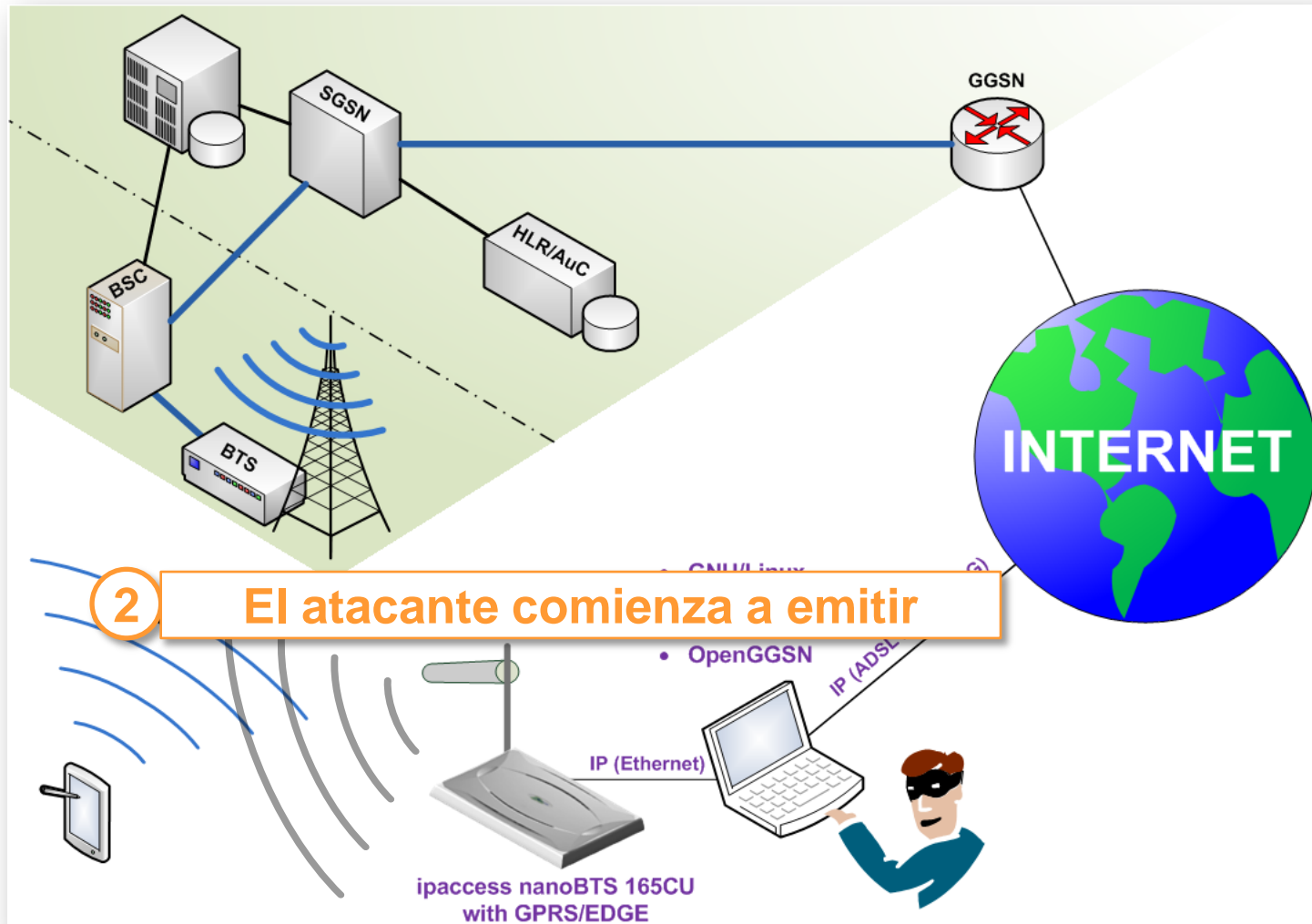
El ataque: punto de partida



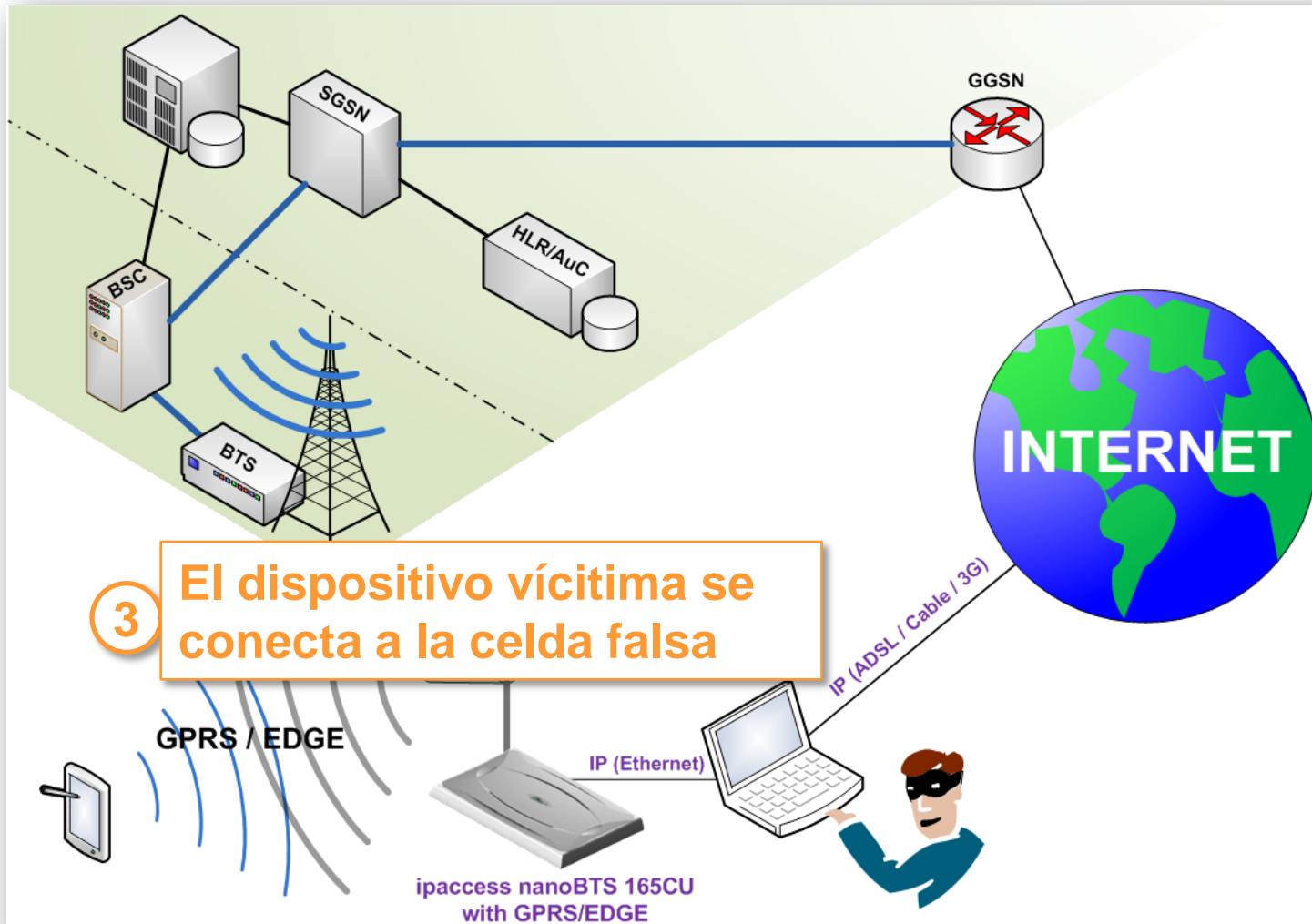
El ataque: paso 1



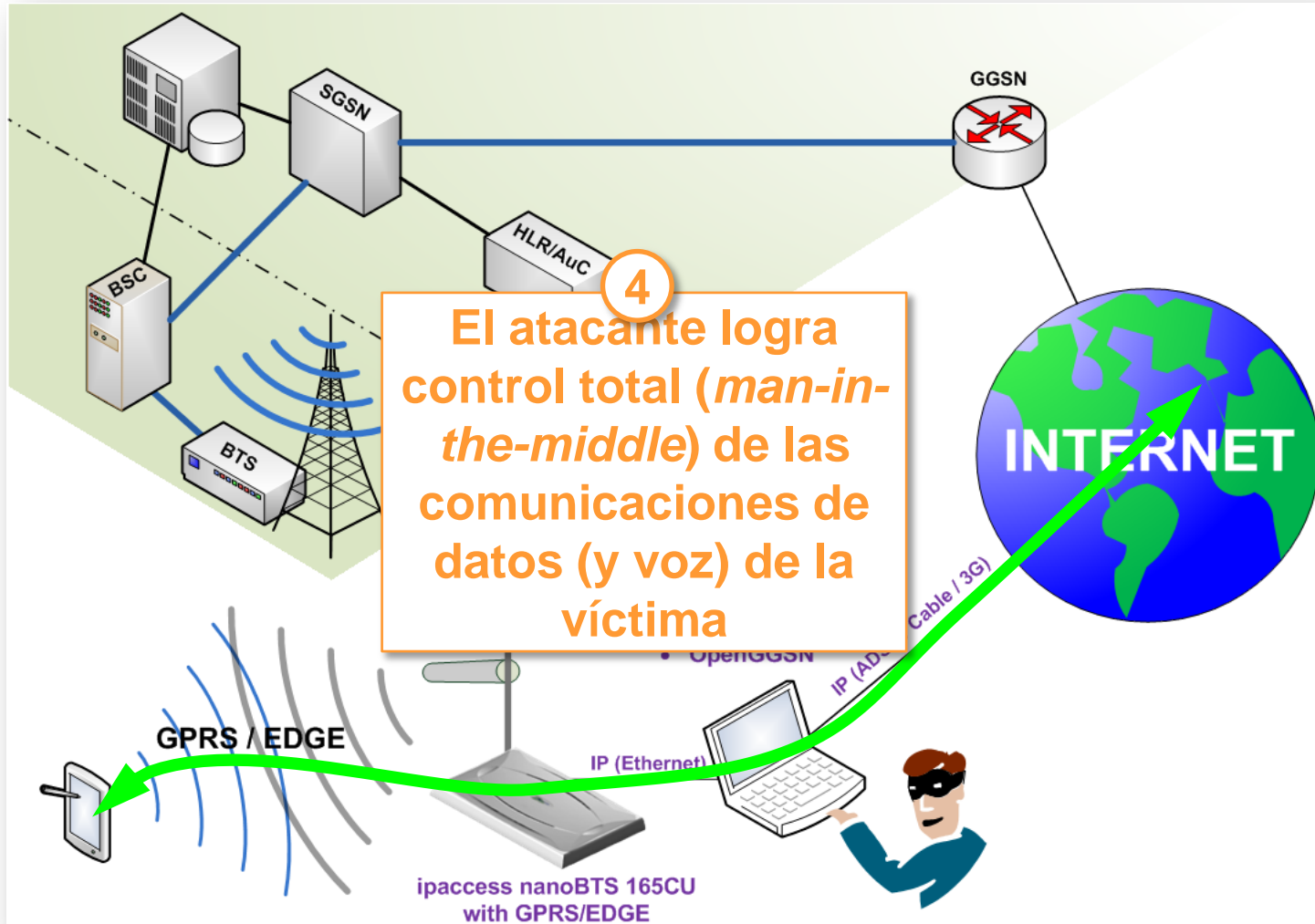
El ataque: paso 2



El ataque: paso 3



El ataque: paso 4



Posición privilegiada del atacante

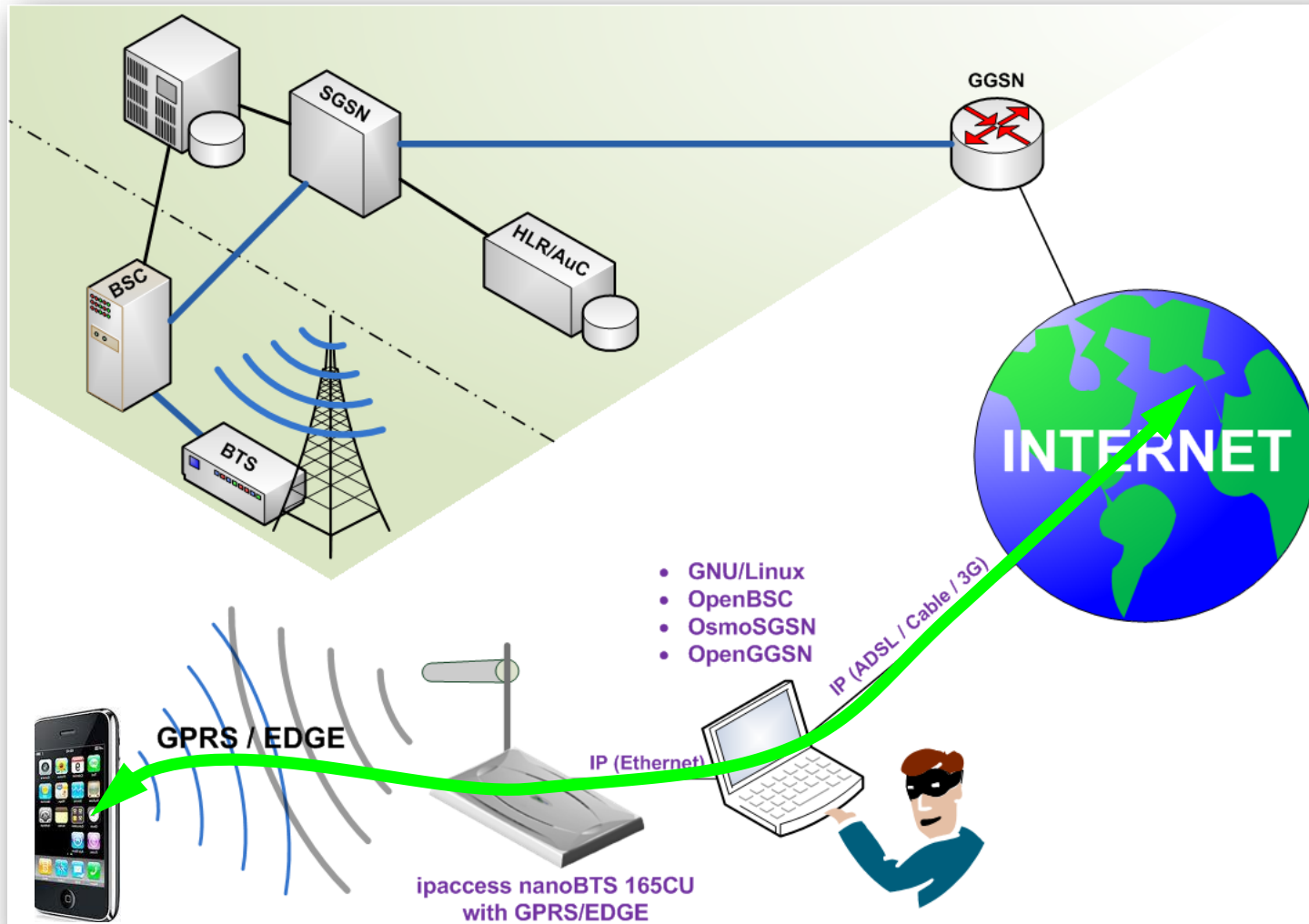


El ataque en acción

Un iPhone cae en la trampa



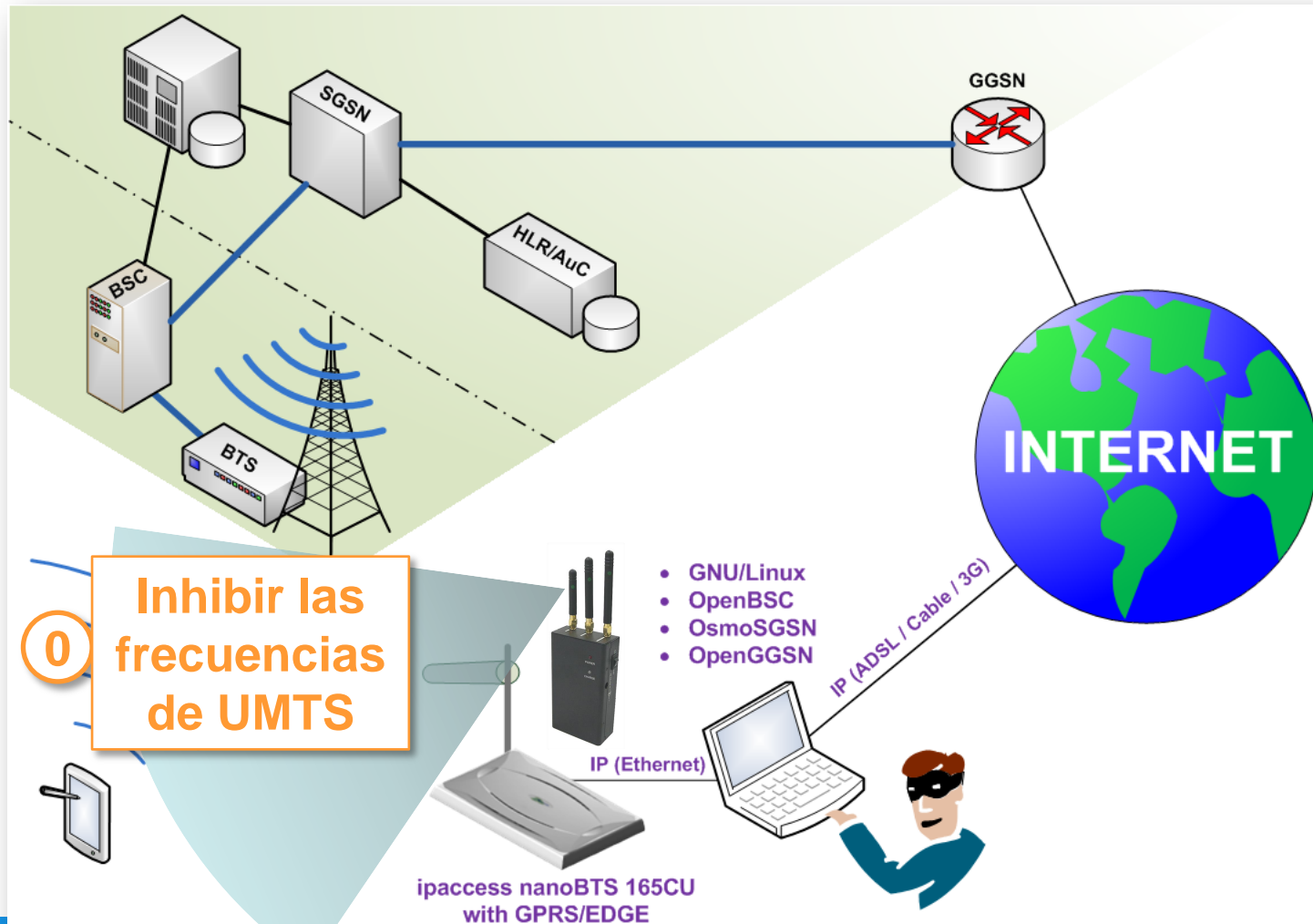
¿Qué ha sucedido?



Extensión del ataque a UMTS

¿Cómo podemos extender este ataque para que sea efectivo contra dispositivos UMTS (3G)?

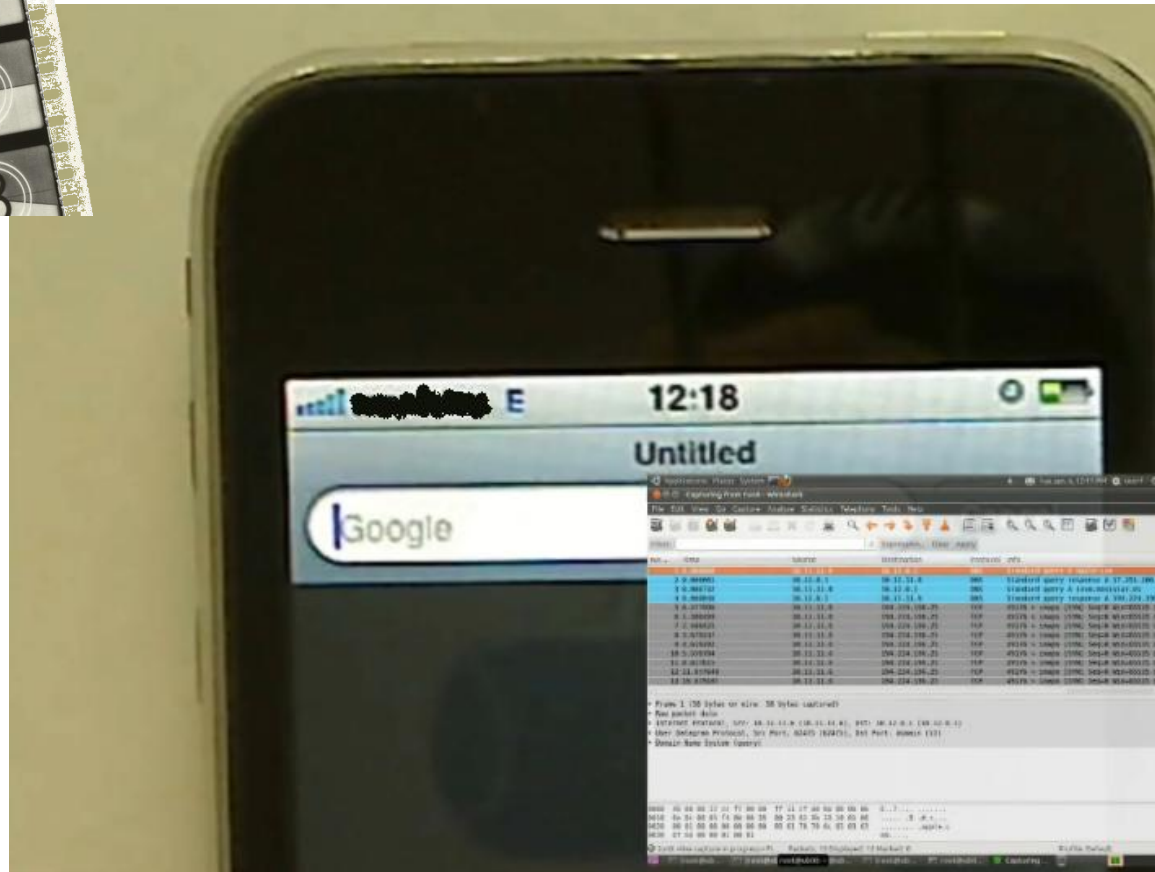
Extensión del ataque a UMTS: Simplemente, añadir un paso previo



Ejemplos de uso del ataque con estación base falsa

Aprovechando el ataque: ejemplo 1

Captura de una búsqueda en Google de un iPhone



¿Qué ha sucedido?

The image shows a Wireshark network traffic capture window. The main pane displays a list of captured packets. Packet 412 is highlighted in red, indicating a duplicate ACK. The packet details pane shows a Domain Name System (query) packet from 10.11.11.6 to 10.12.0.1. The raw packet data pane shows the hex and ASCII representation of the packet. A green arrow points from the highlighted packet to a globe labeled 'INTERNET'. Below the Wireshark window, a diagram shows a smartphone connected to a laptop via a network interface. The smartphone is labeled 'GPRS / EDGE' and the laptop is labeled 'IP (Ethernet)'. The network interface is labeled 'ipaccess nanoBTS 165CU with GPRS/EDGE'. A person in a blue shirt and red mask is holding the laptop.

No.	Time	Source	Destination	Protocol	Info
409	58.540863	87.186.205.101	10.11.11.6	TCP	http > 49186 [FIN, ACK] Seq=9513 Ack=...
410	58.922581	10.11.11.6	173.194.37.104	TCP	49185 > http [ACK] Seq=1144 Ack=549 W...
411	58.922723	10.11.11.6	87.186.205.101	TCP	49189 > http [ACK] Seq=1494 Ack=9800 ...
412	58.942620	10.11.11.6	87.186.205.101	TCP	[TCP Dup ACK 403#1] 49188 > http [ACK]
413	58.942185	10.11.11.6	87.186.205.101	TCP	49186 > http [ACK] Seq=2805 Ack=9514 ...
414	59.479399	10.11.11.6	194.224.196.25	TCP	49190 > imap [SYN] Seq=0 Win=65535 Le...
415	60.518596	10.11.11.6	194.224.196.25	TCP	49190 > imap [SYN] Seq=0 Win=65535 Le...
416	61.847016	10.11.11.6	194.224.196.25	TCP	49190 > imap [SYN] Seq=0 Win=65535 Le...
417	62.779089	10.11.11.6	194.224.196.25	TCP	49190 > imap [SYN] Seq=0 Win=65535 Le...
418	63.697499	10.11.11.6	194.224.196.25	TCP	49190 > imap [SYN] Seq=0 Win=65535 Le...
419	66.778060	10.11.11.6	194.224.196.25	TCP	49190 > imap [SYN] Seq=0 Win=65535 Le...
420	69.833199	10.11.11.6	194.224.196.25	TCP	49190 > imap [SYN] Seq=0 Win=65535 Le...
421	77.888696	10.11.11.6	194.224.196.25	TCP	49190 > imap [SYN] Seq=0 Win=65535 Le...

Frame 1 (58 bytes on wire, 58 bytes captured)
Raw packet data
Internet Protocol, Src: 10.11.11.6 (10.11.11.6), Dst: 10.12.0.1 (10.12.0.1)
User Datagram Protocol, Src Port: 62475 (62475), Dst Port: domain (53)
Domain Name System (query)

0000 45 00 00 37 cc f7 00 00 ff 11 cf a0 0a 0b 0b 06 E..7.....
0010 0a 0c 00 01 f4 0b 00 35 00 23 81 2b 13 16 01 005.#+...
0020 00 01 00 00 00 00 00 00 05 61 70 70 6c 65 03 63apple.c
0030 6f 6d 00 00 01 00 01 om.....

tun0: <live capture in progress> Fl... = Packets: 421 Displayed: 421 Marked: 0 Profile: Default

GPRS / EDGE

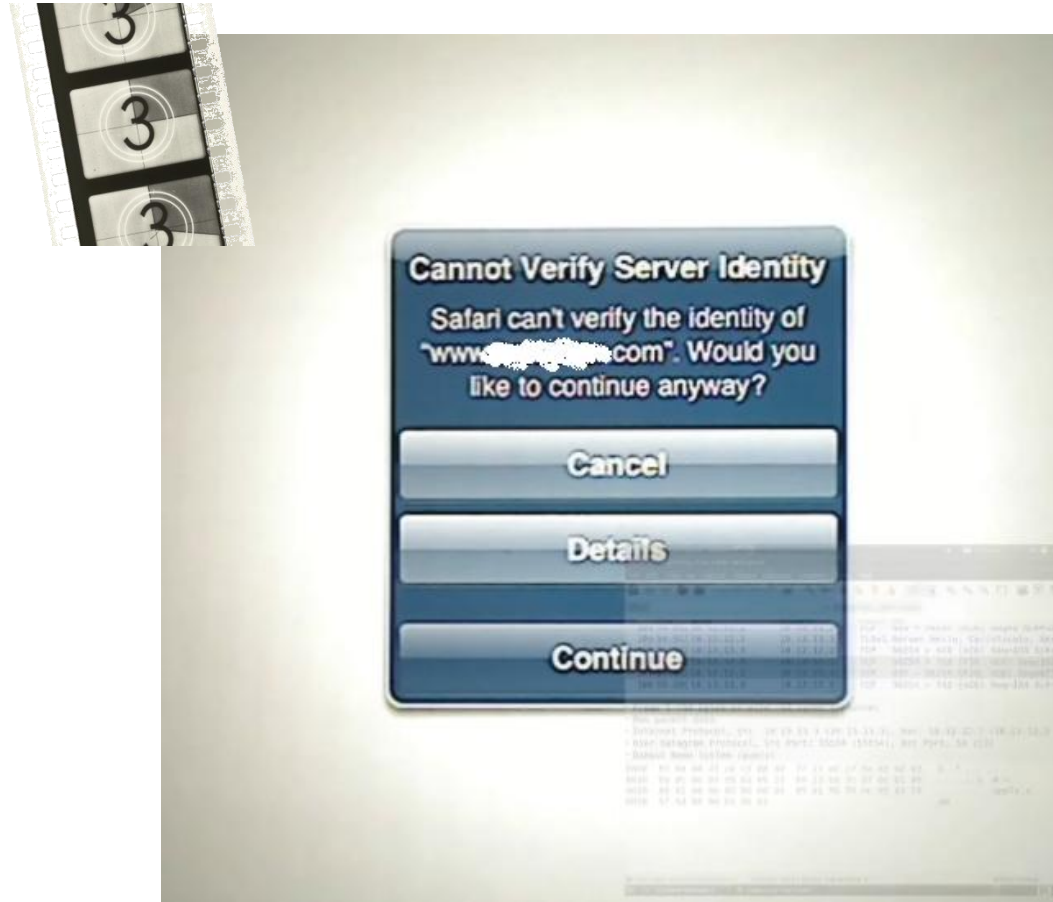
IP (Ethernet)

ipaccess nanoBTS 165CU with GPRS/EDGE

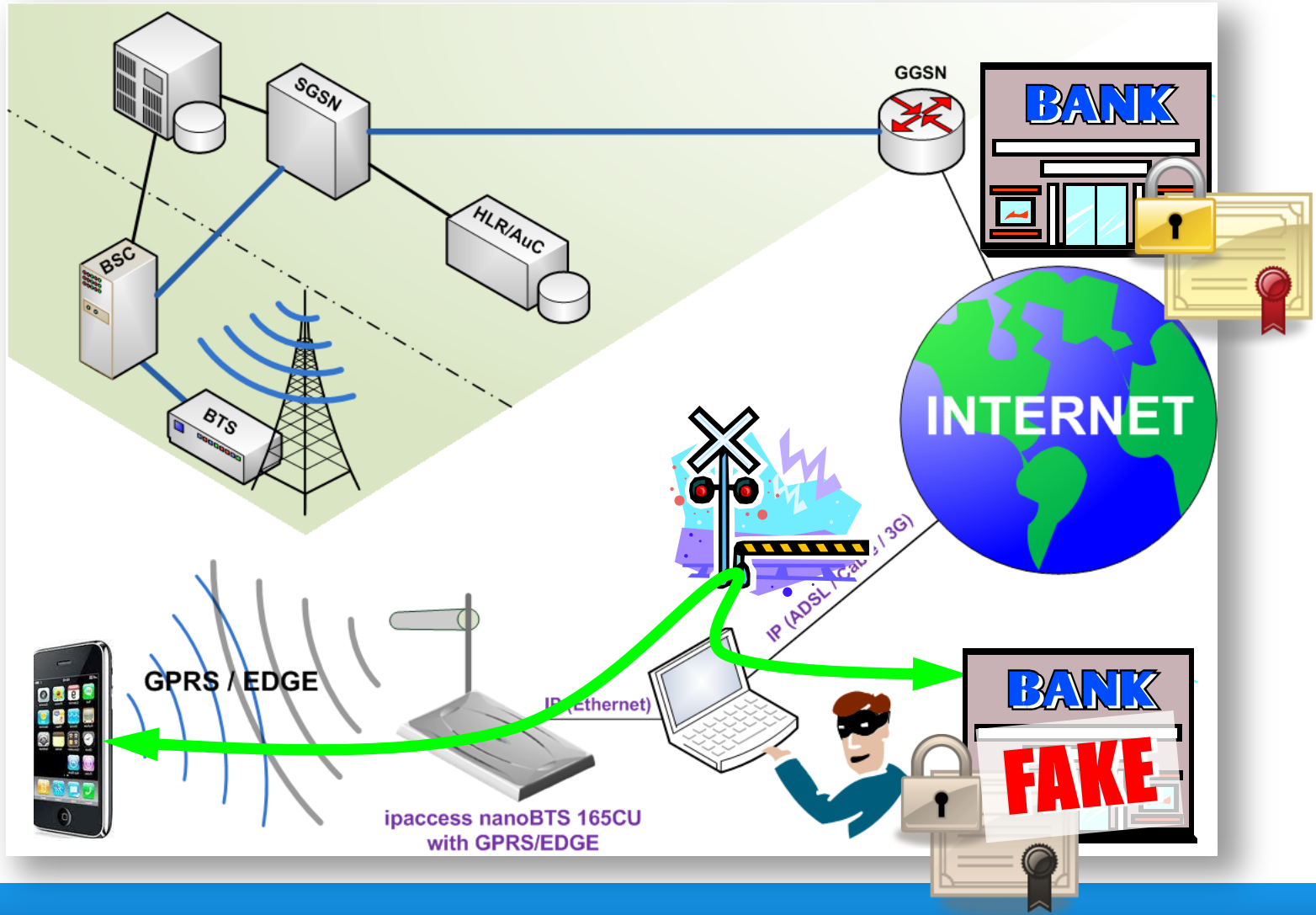
INTERNET

Aprovechando el ataque: ejemplo 2

Ataque de phishing contra un iPad (usando https)



¿Qué ha sucedido?

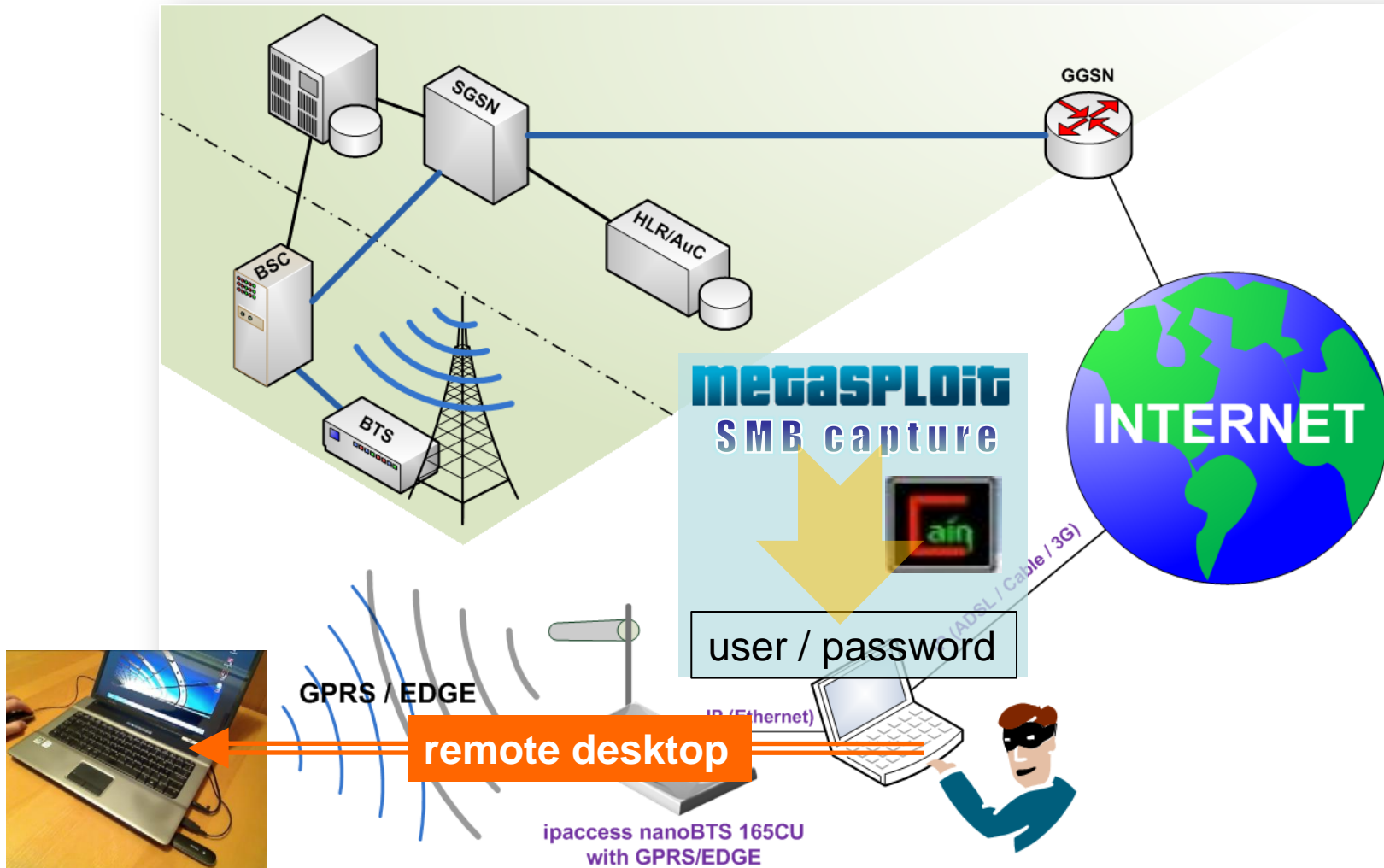


Aprovechando el ataque: ejemplo 3

Toma de control de un PC a través de GPRS/EDGE



¿Qué ha sucedido?

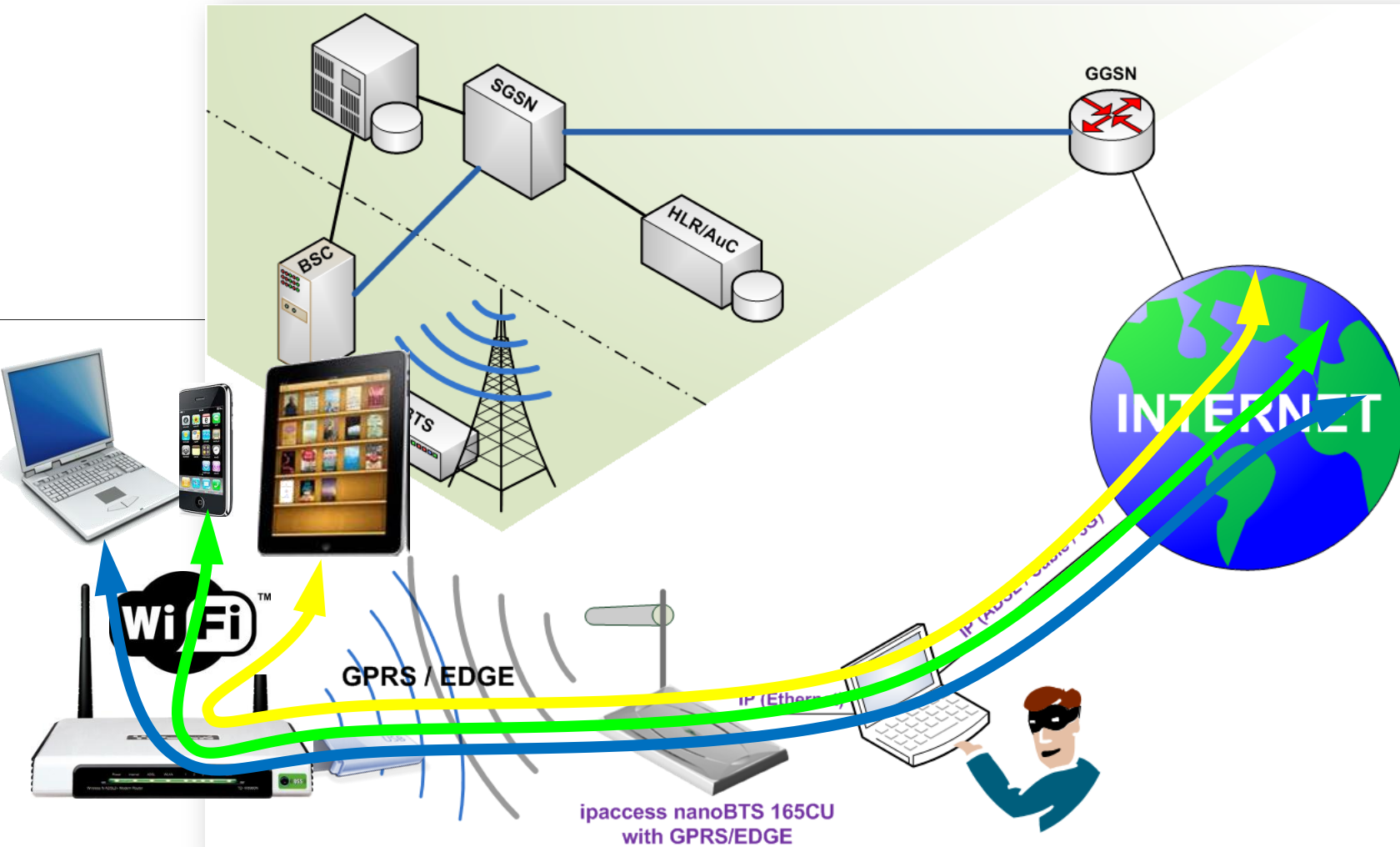


Aprovechando el ataque: ejemplo 4

Control del tráfico de todos los dispositivos ubicados tras un router 3G



¿Qué ha sucedido?

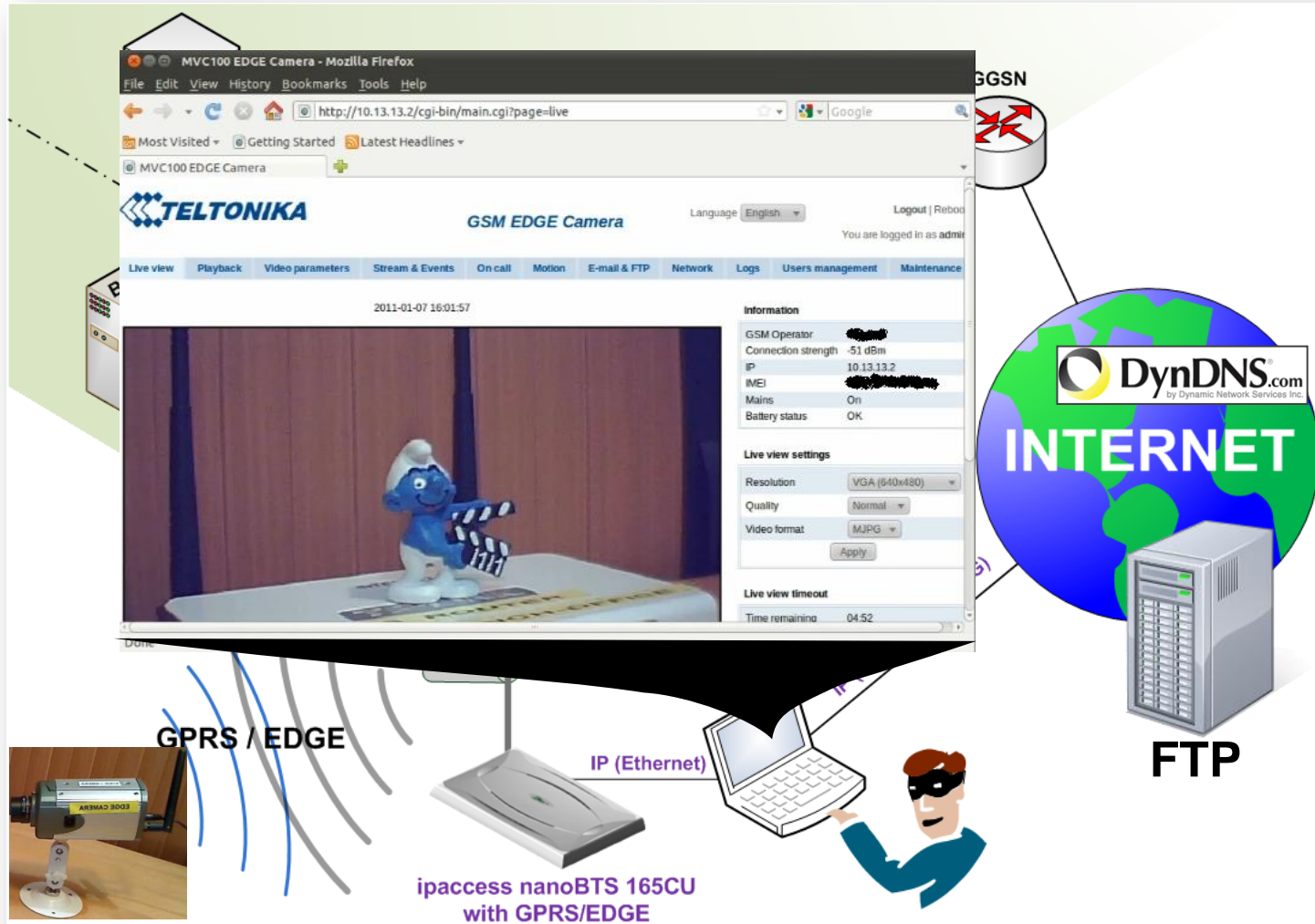


Aprovechando el ataque: ejemplo 5

Ataques contras otro dispositivos GPRS/EDGE



¿Qué ha sucedido?



The slide features a white background with decorative blue and black elements. A thick black horizontal line is positioned above the title, extending from the left edge towards the center. Another thick black horizontal line is positioned below the title, extending from the center towards the right edge. The text 'Medidas de protección' is centered between these two lines. The bottom of the slide has a solid blue background.

Medidas de protección

Medidas de protección

- Configurar nuestros dispositivos móviles para aceptar sólo 3G, rechazando 2G
- Cifrar nuestras comunicaciones de datos en niveles superiores (HTTPS, SSH, IPSEC, etc.)
- Instalar y configurar un firewall software en nuestros dispositivos móviles

Medidas de protección

- Diseñar las formas de acceso a nuestras aplicaciones en la nube teniendo en cuenta los vectores de ataque contra comunicaciones móviles existentes

Acceso móvil a la nube: un punto vulnerable

David Pérez

david@taddong.com

José Picó

jose@taddong.com

Twitter: @taddong

IX Foro de Seguridad - RedIRIS

Valencia, 10 de Marzo de 2011