Acceso móvil a la nube: un punto vulnerable

David Pérez

José Picó

IX Foro de Seguridad - RedIRIS

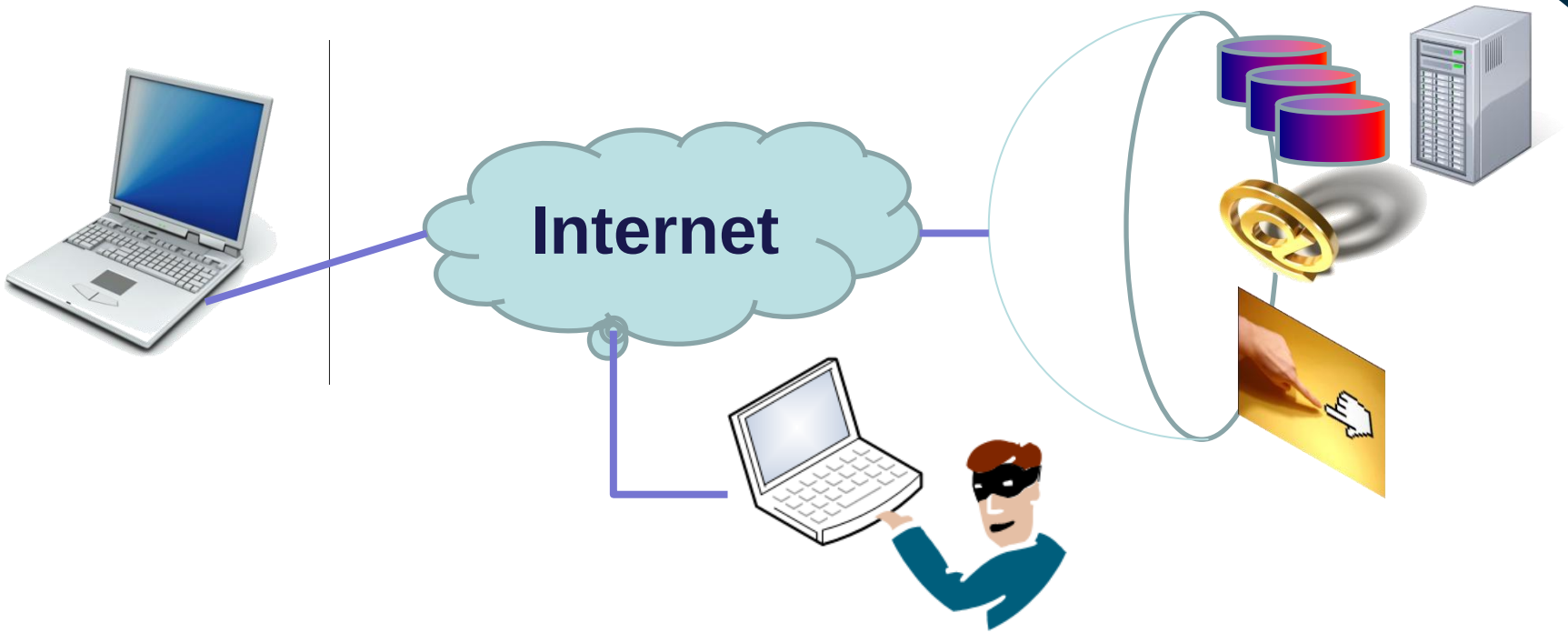
Valencia, 10 de Marzo de 2011

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

Riesgos en los accesos móviles a la nube

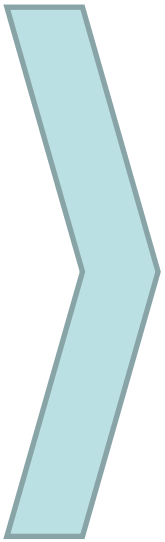
Riesgos en el acceso a los servicios en la nube



- 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

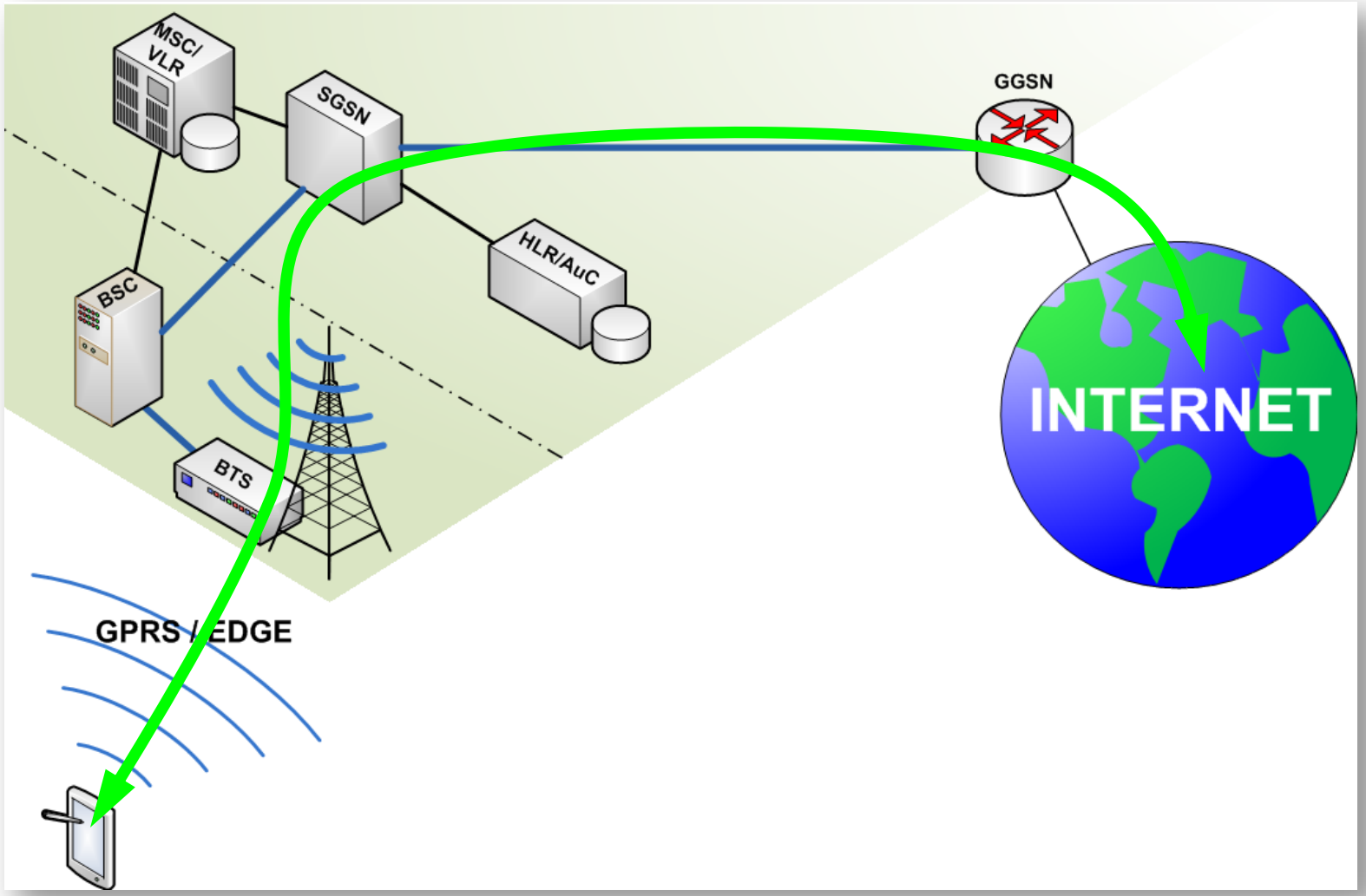
- Riesgos adicionales de un móvil:
  - Otras conexiones normalmente habilitadas (WiFi, bluetooth)
  - No suele disponer de software de cifrado, VPN, firewall, etc.
  - 2G/3G: canal adicional de comunicaciones, normalmente no contemplado en las acciones preventivas de la seguridad de las organizaciones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

Posibles ataques a comunicaciones móviles de datos

Arquitectura GPRS/EDGE

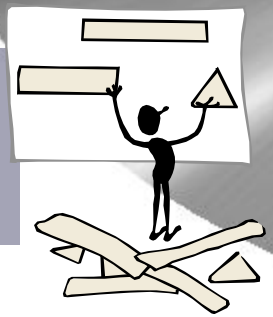


Comunicaciones móviles expuestas a varios vectores de ataque

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.acccess (*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*)

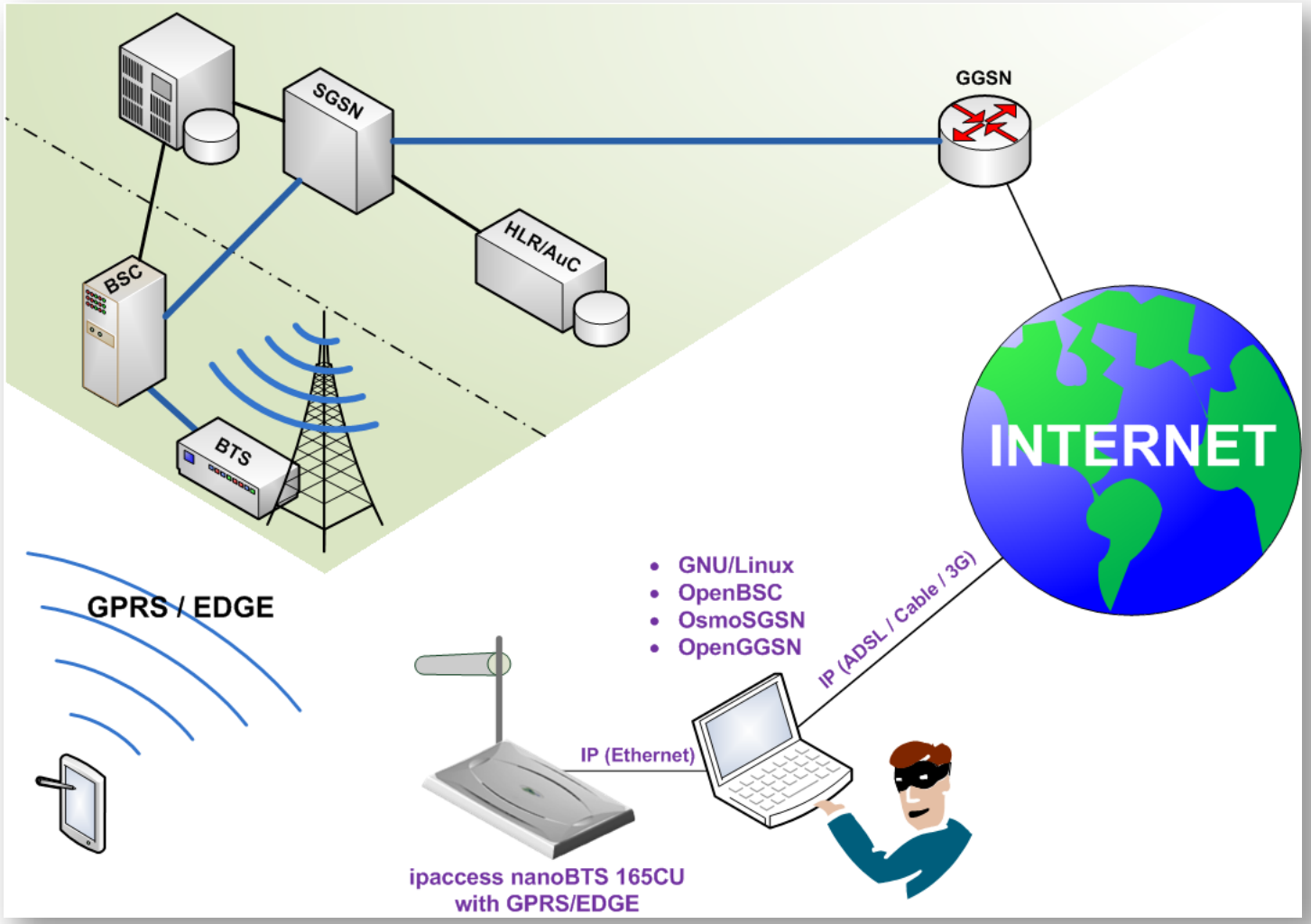
- Capaz de inhibir las frecuencias asignadas a UMTS/HSPA en un lugar determinado, sin perturbar las frecuencias de GSM/GPRS/EDGE

"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."

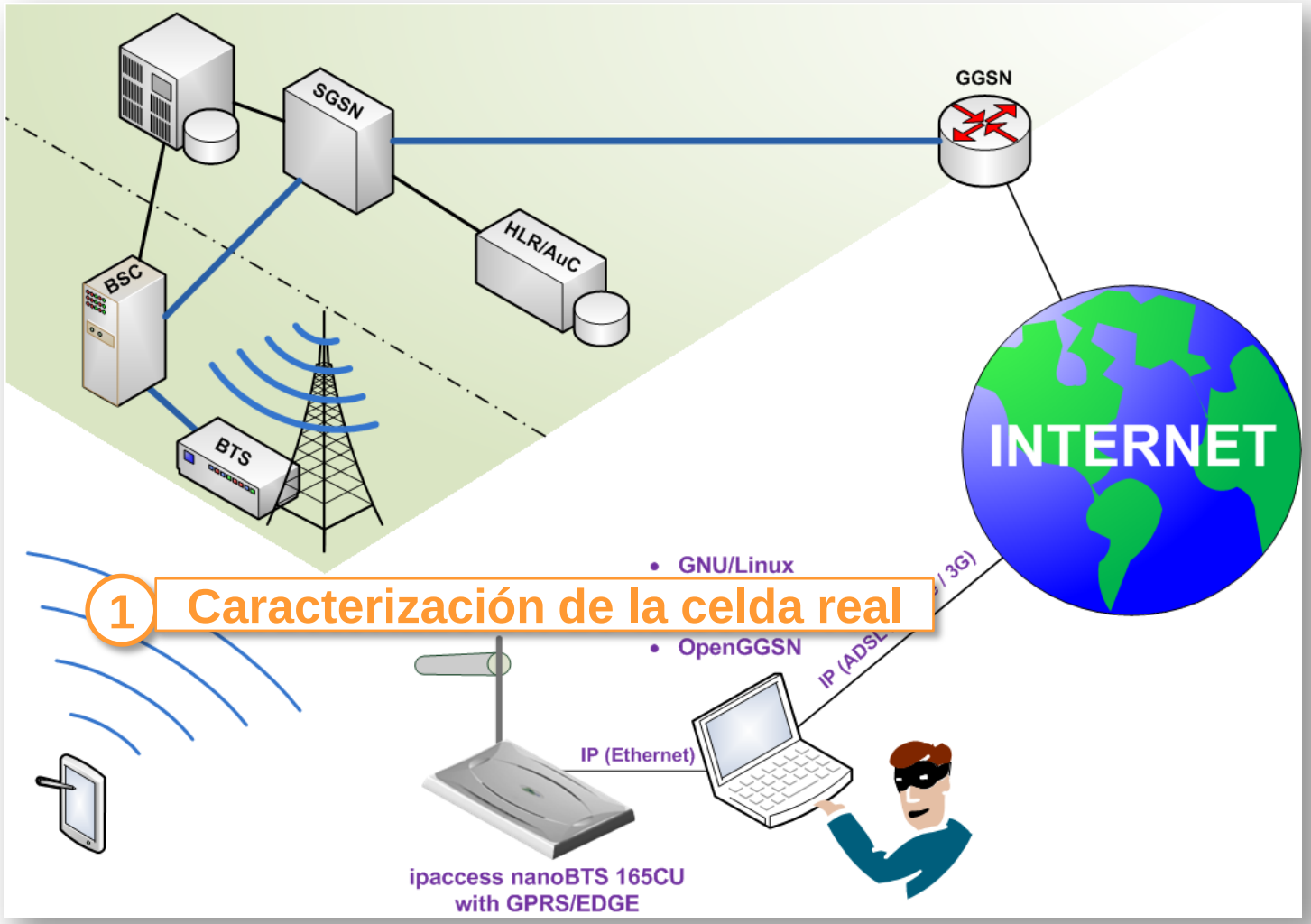
[Source: Wikipedia]

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

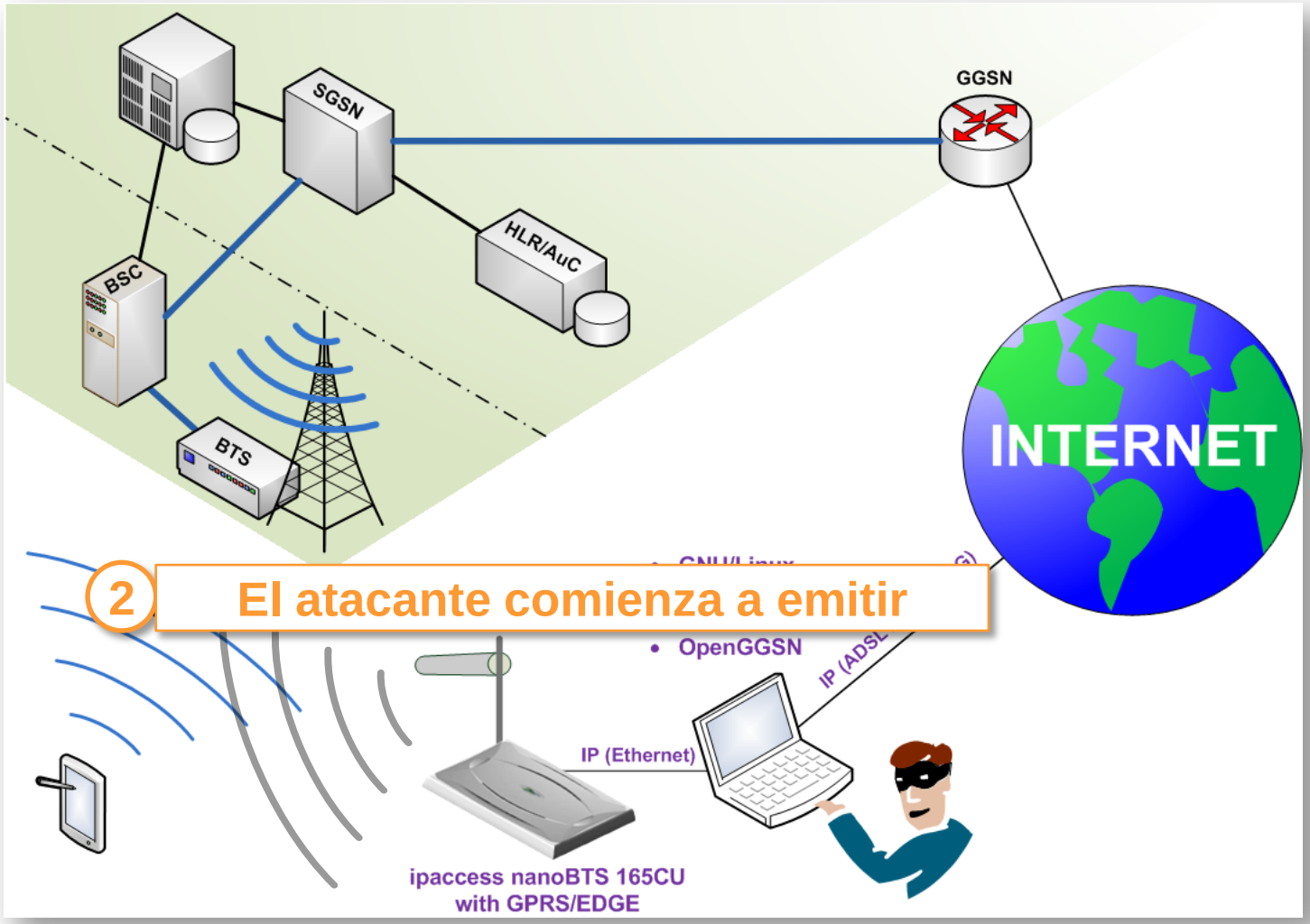
El ataque: punto de partida



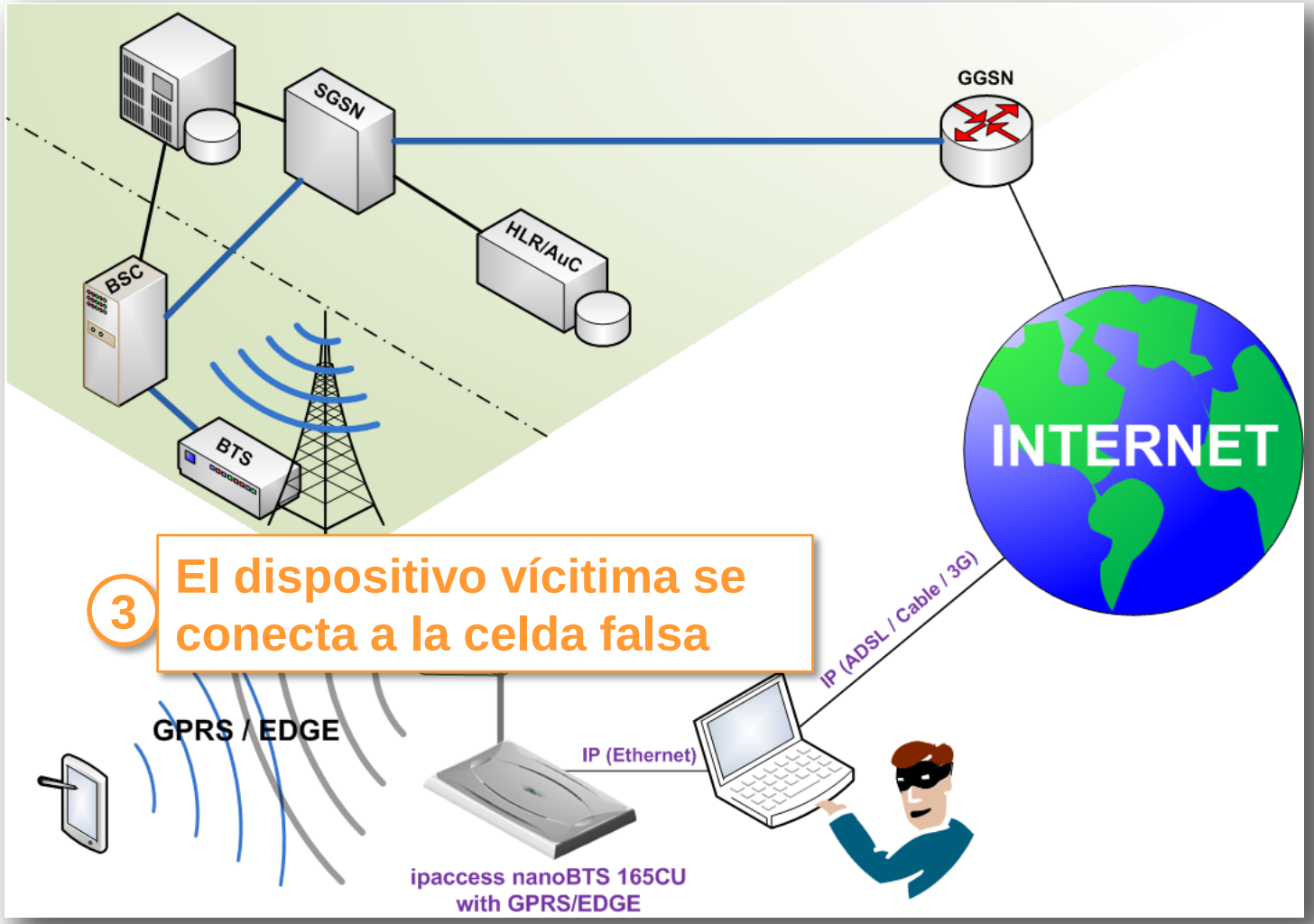
El ataque: paso 1



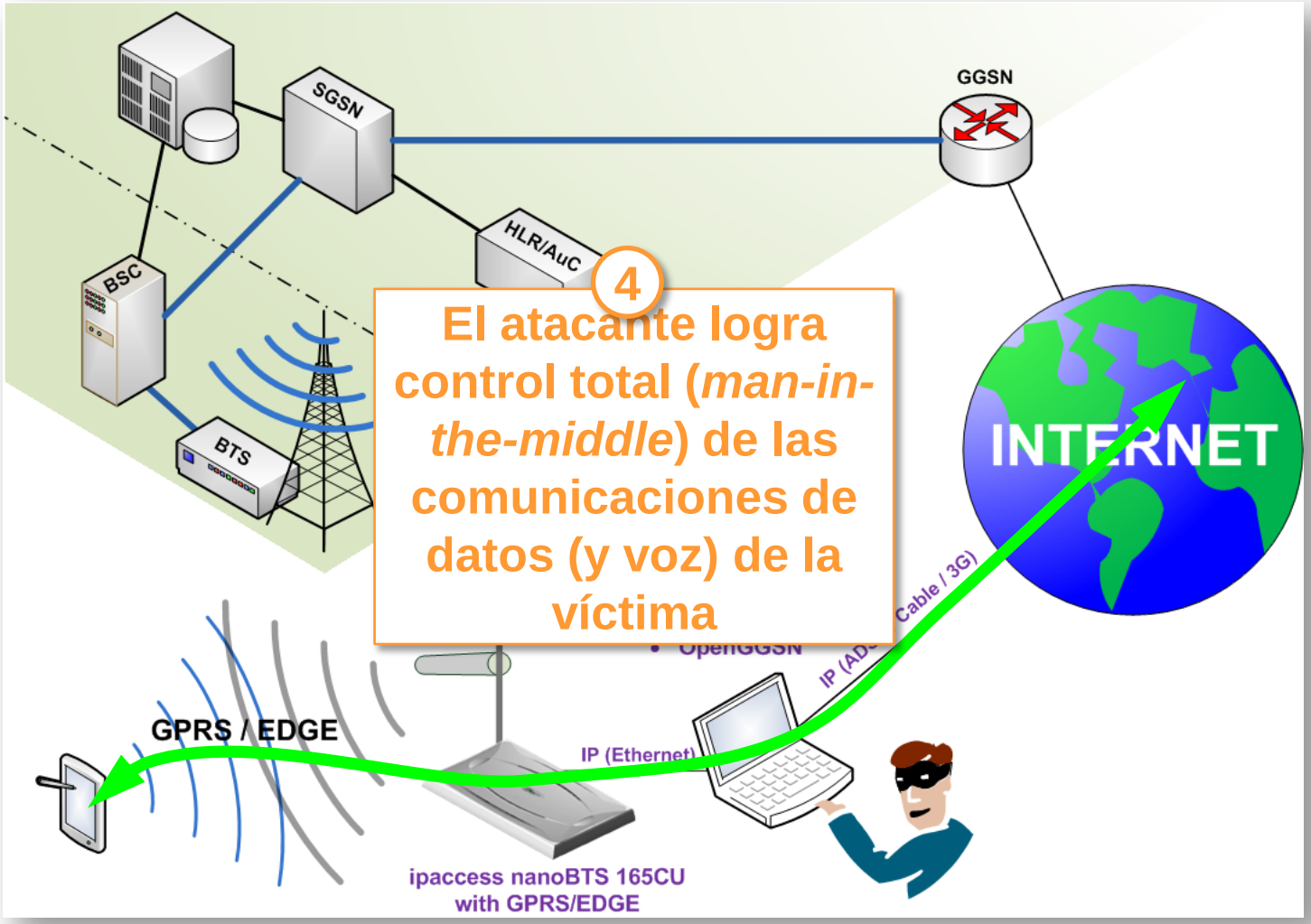
El ataque: paso 2



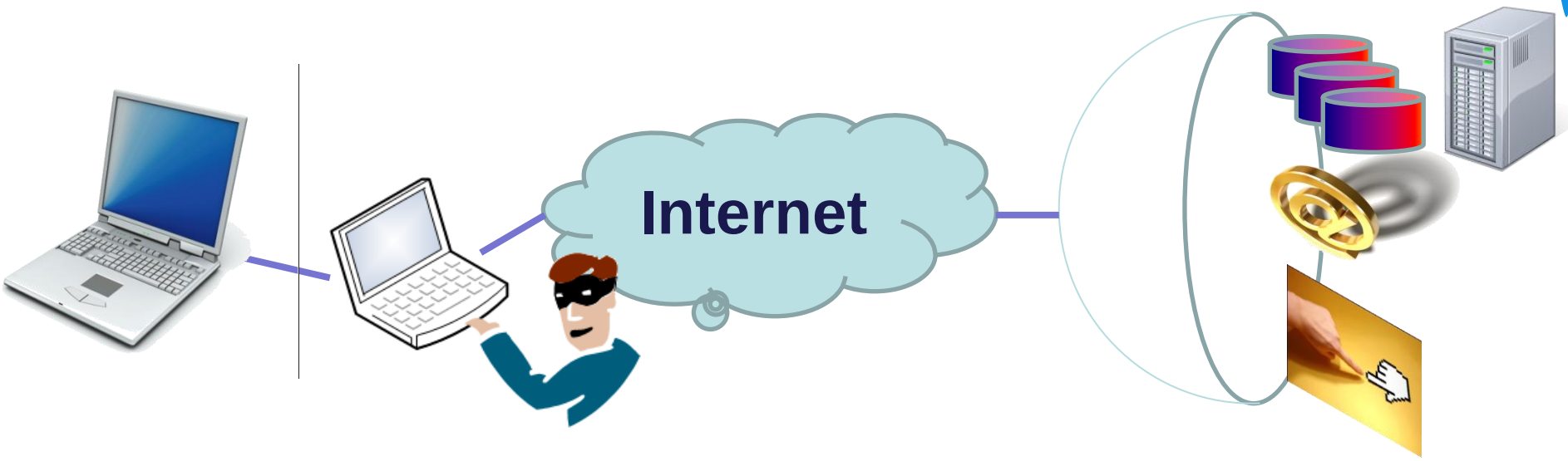
El ataque: paso 3



El ataque: paso 4

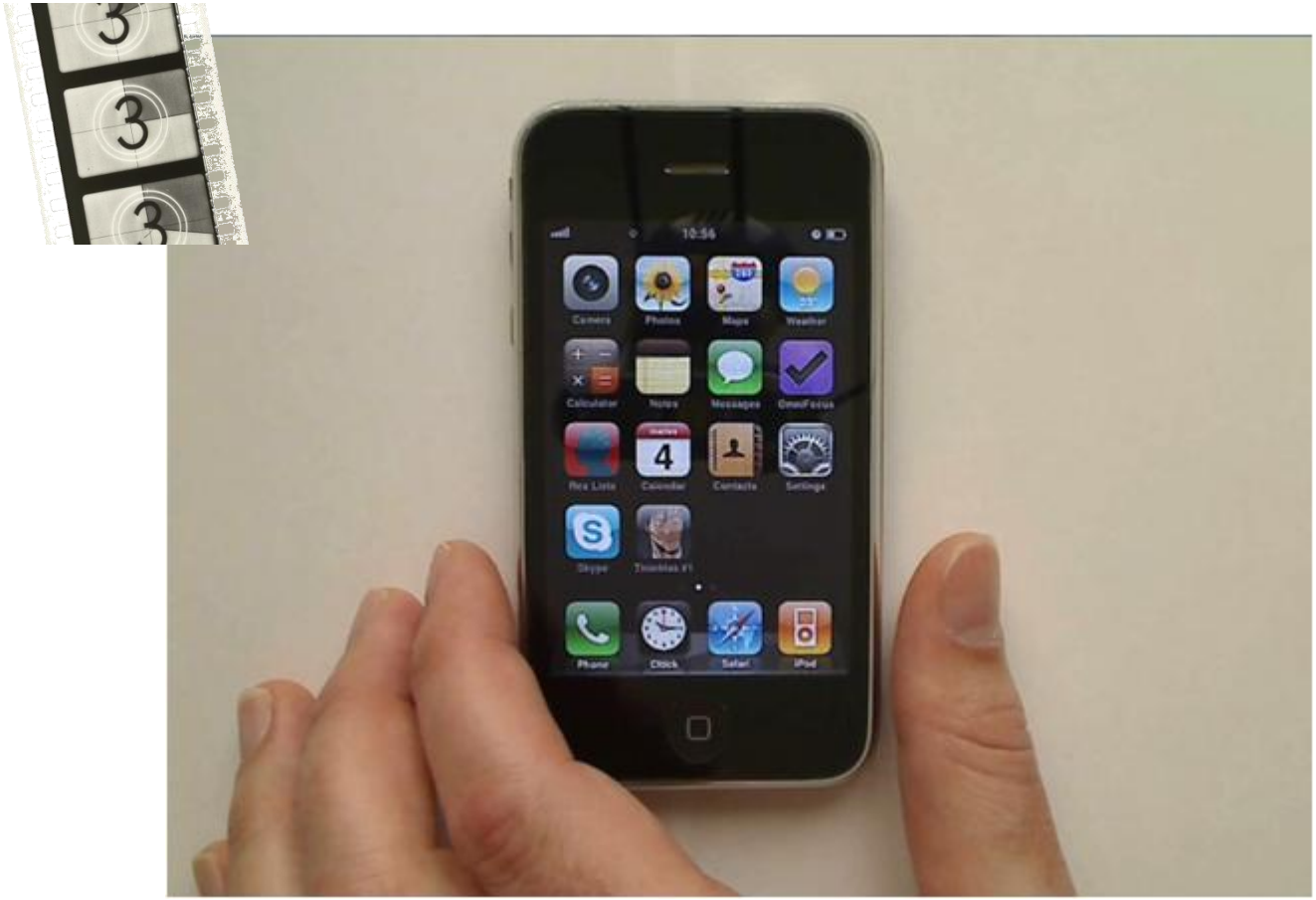


Posición privilegiada del atacante

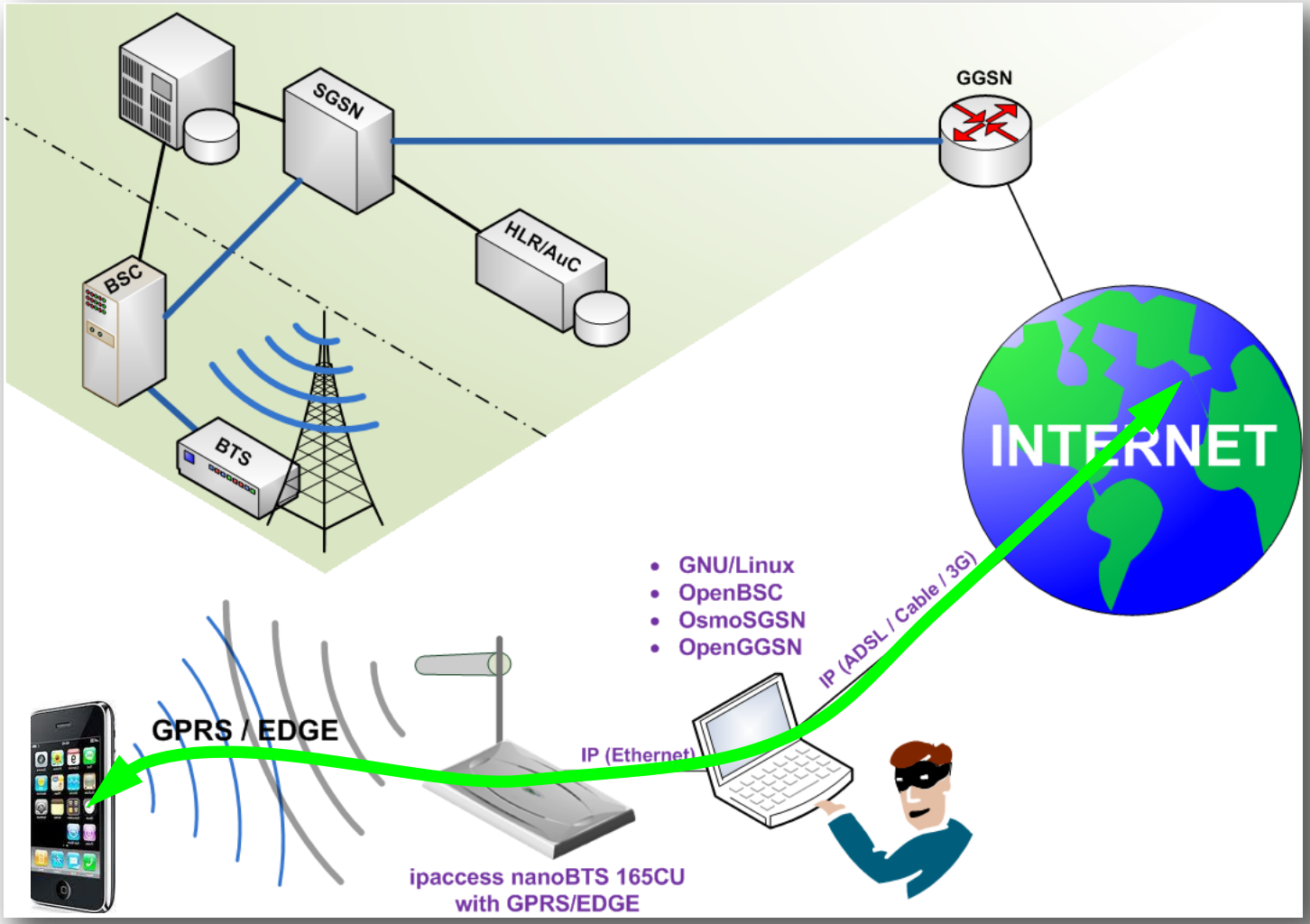


El ataque en acción

Un iPhone cae en la trampa



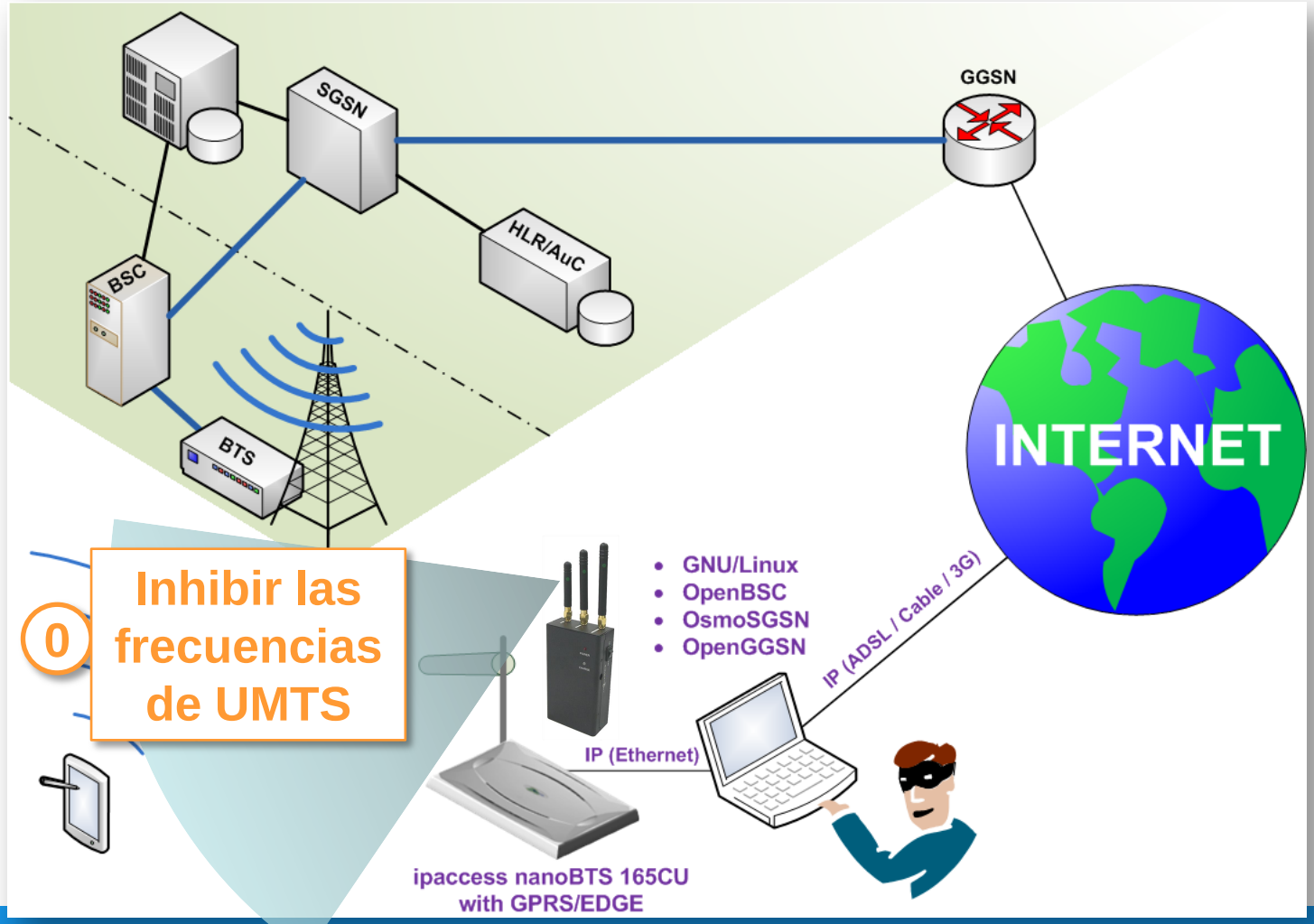
¿Qué ha sucedido?



Extensión del ataque a UMTS

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

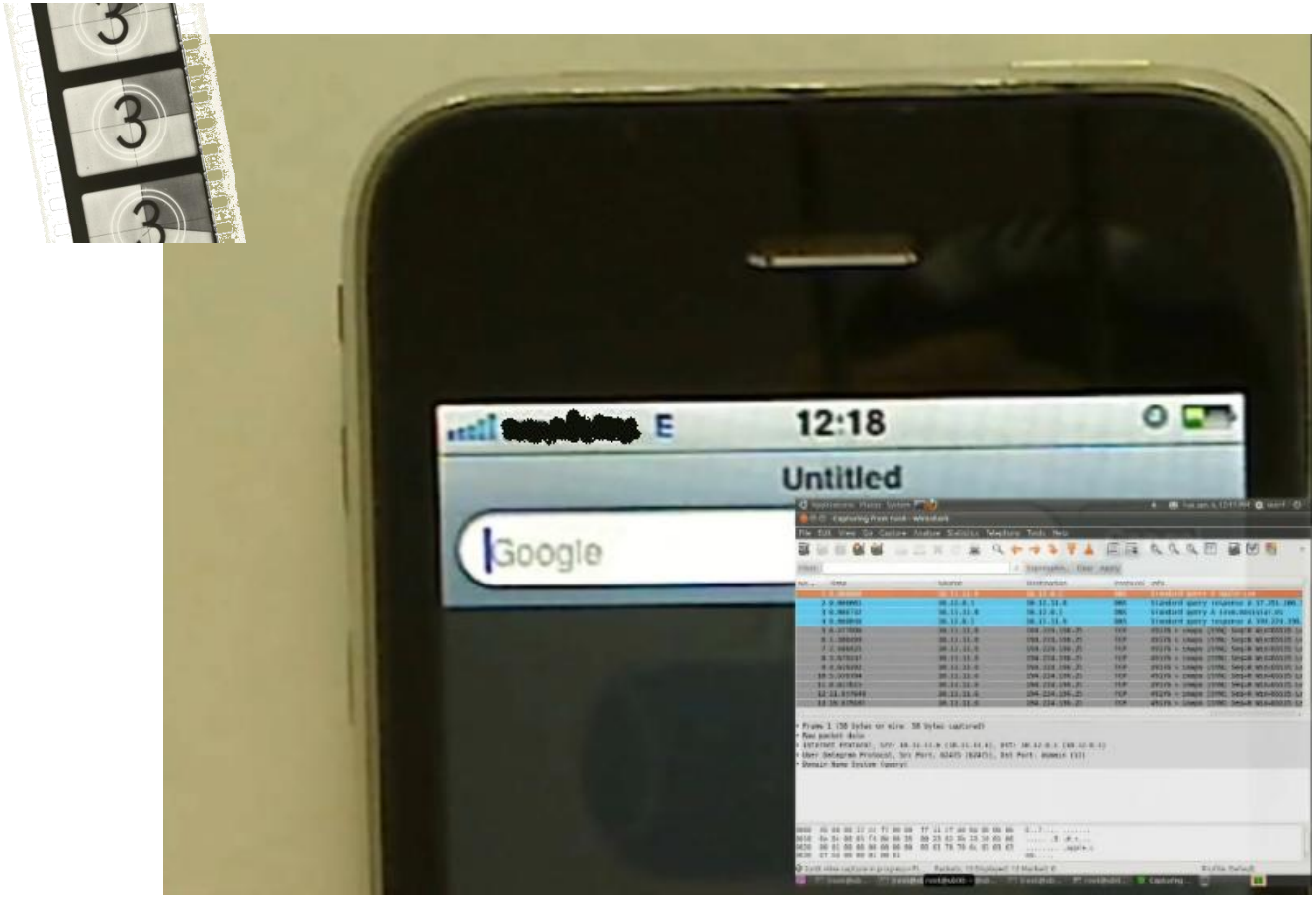
Extensión del ataque a UMTS: Simplemente, añadir un paso previo



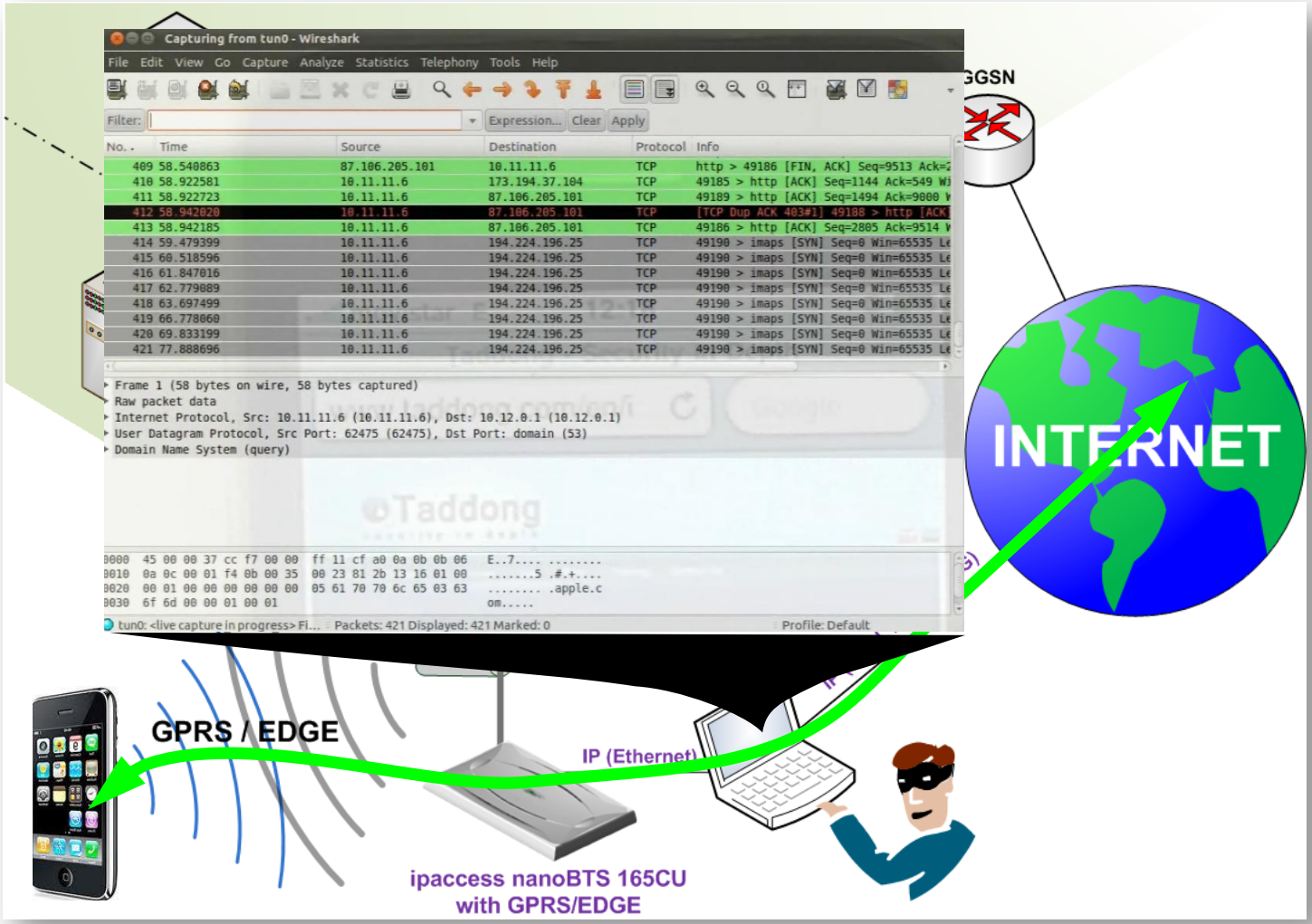
Ejemplos de uso del ataque con estación base falsa

Aprovechando el ataque: ejemplo 1

Captura de una búsqueda en Google de un iPhone

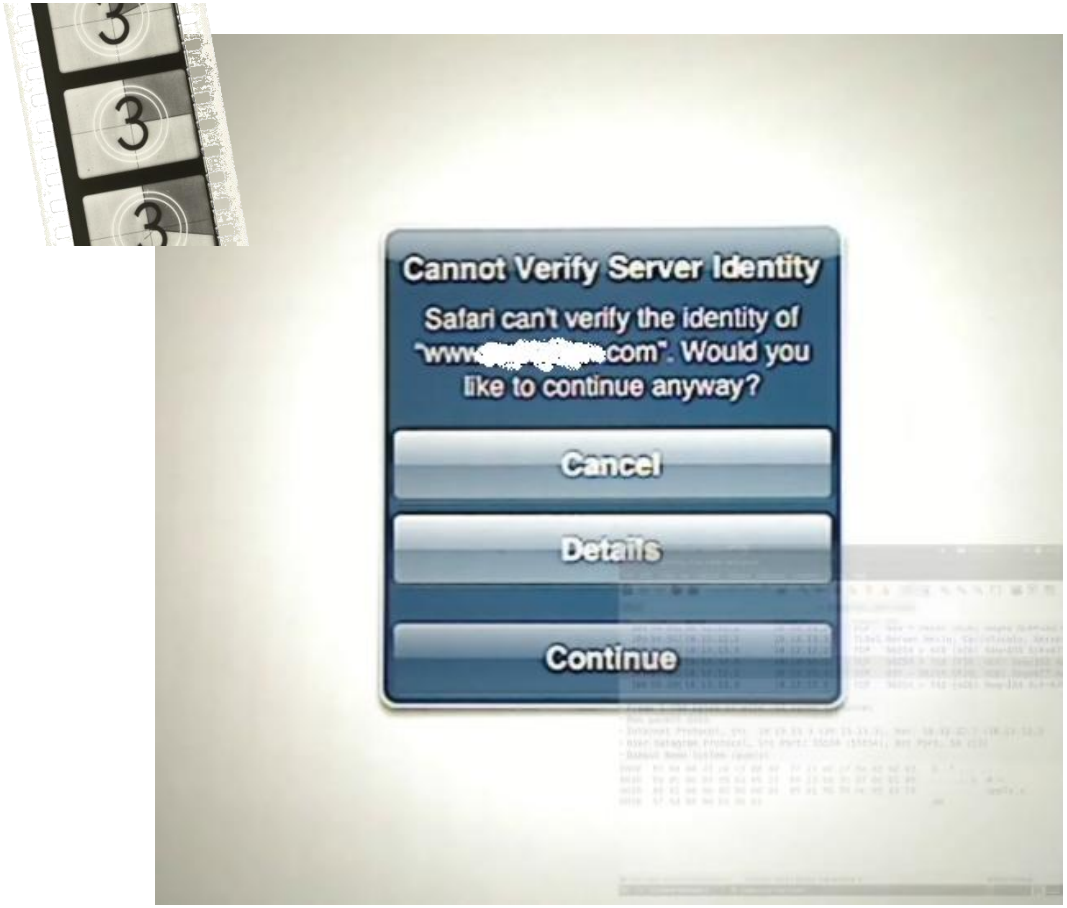


¿Qué ha sucedido?

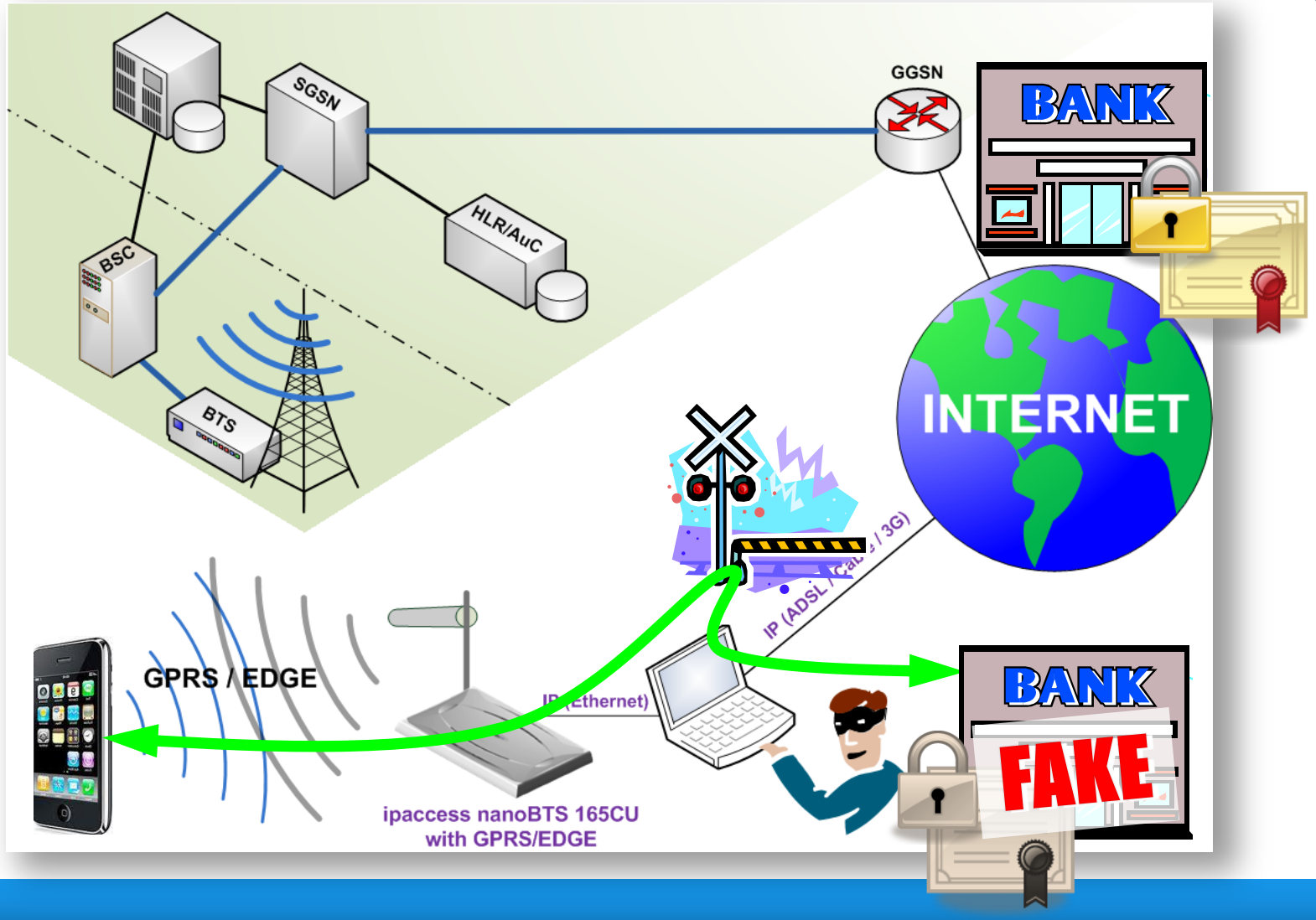


Aprovechando el ataque: ejemplo 2

Ataque de phishing contra un iPad (usando https)



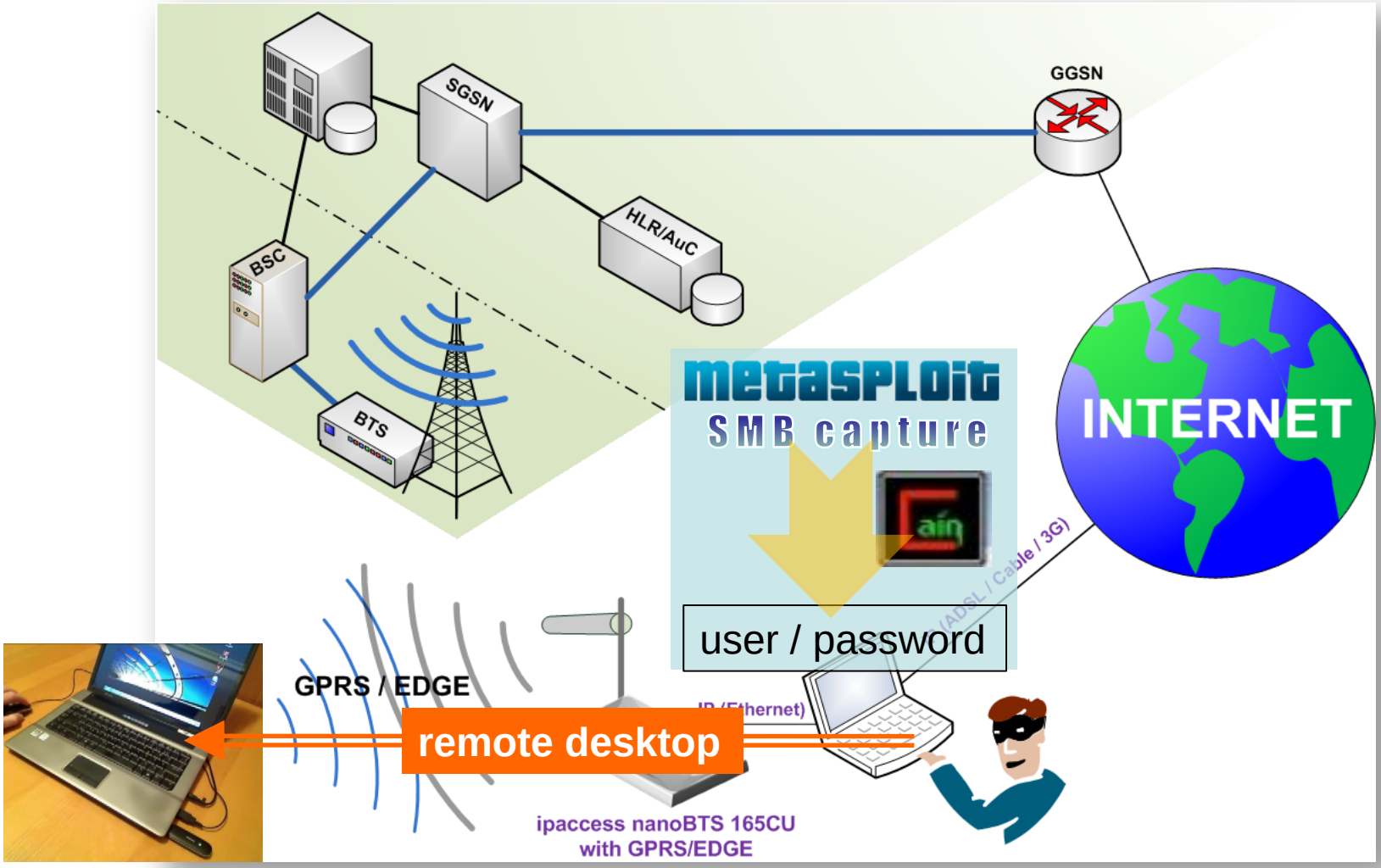
¿Qué ha sucedido?



Aprovechando el ataque: ejemplo 3

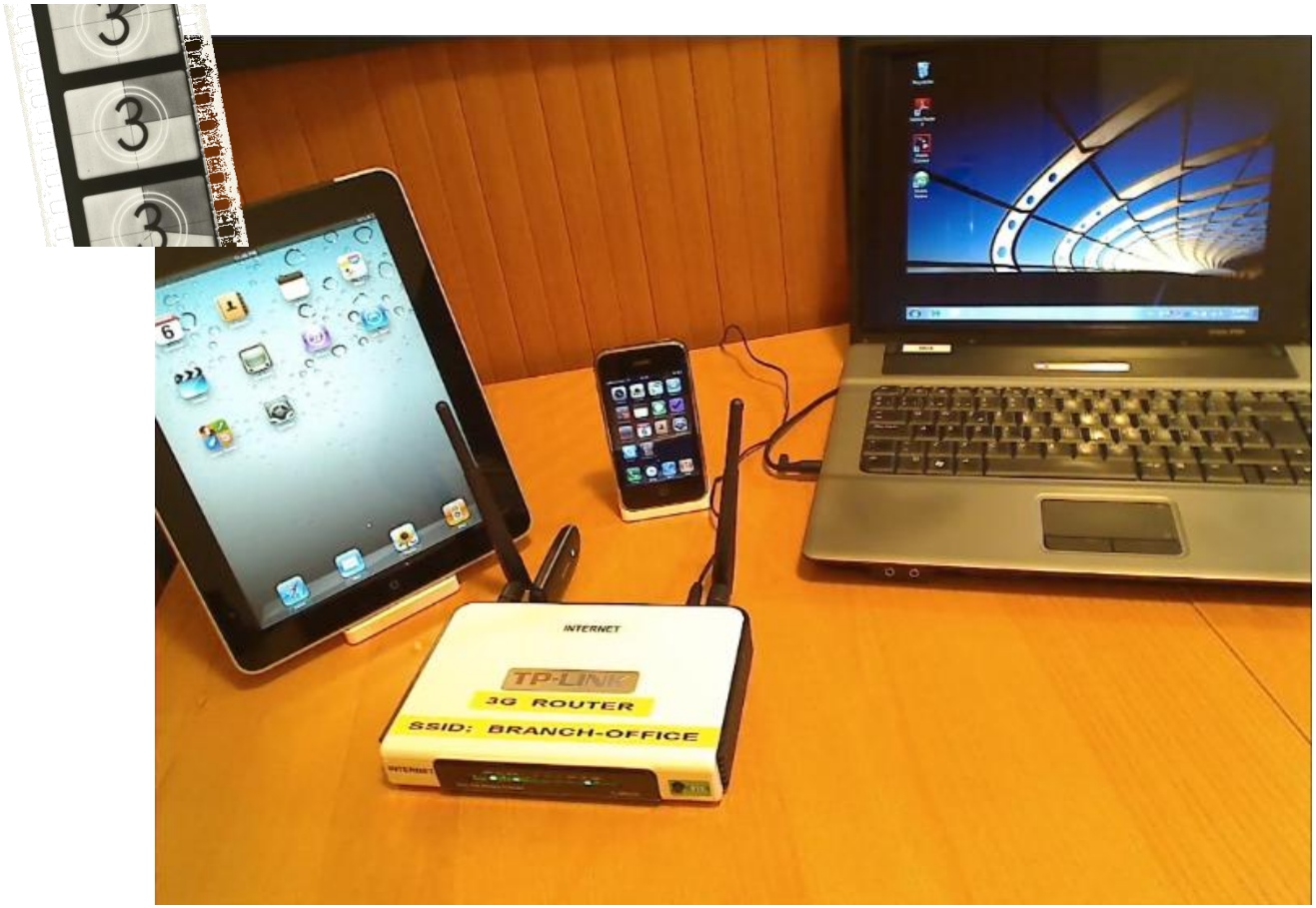
Toma de control de un PC a través de GPRS/EDGE

¿Qué ha sucedido?

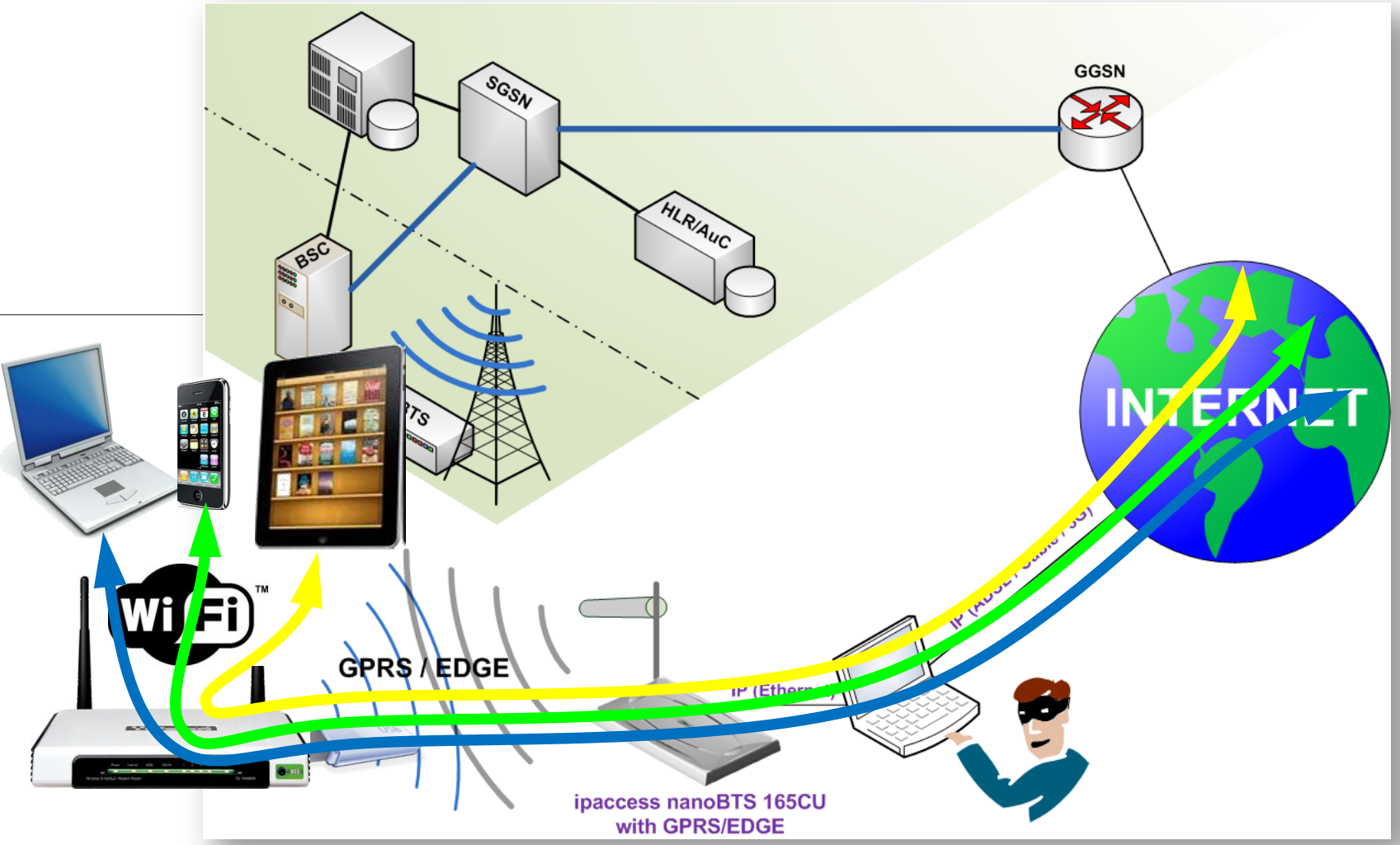


Aprovechando el ataque: ejemplo 4

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



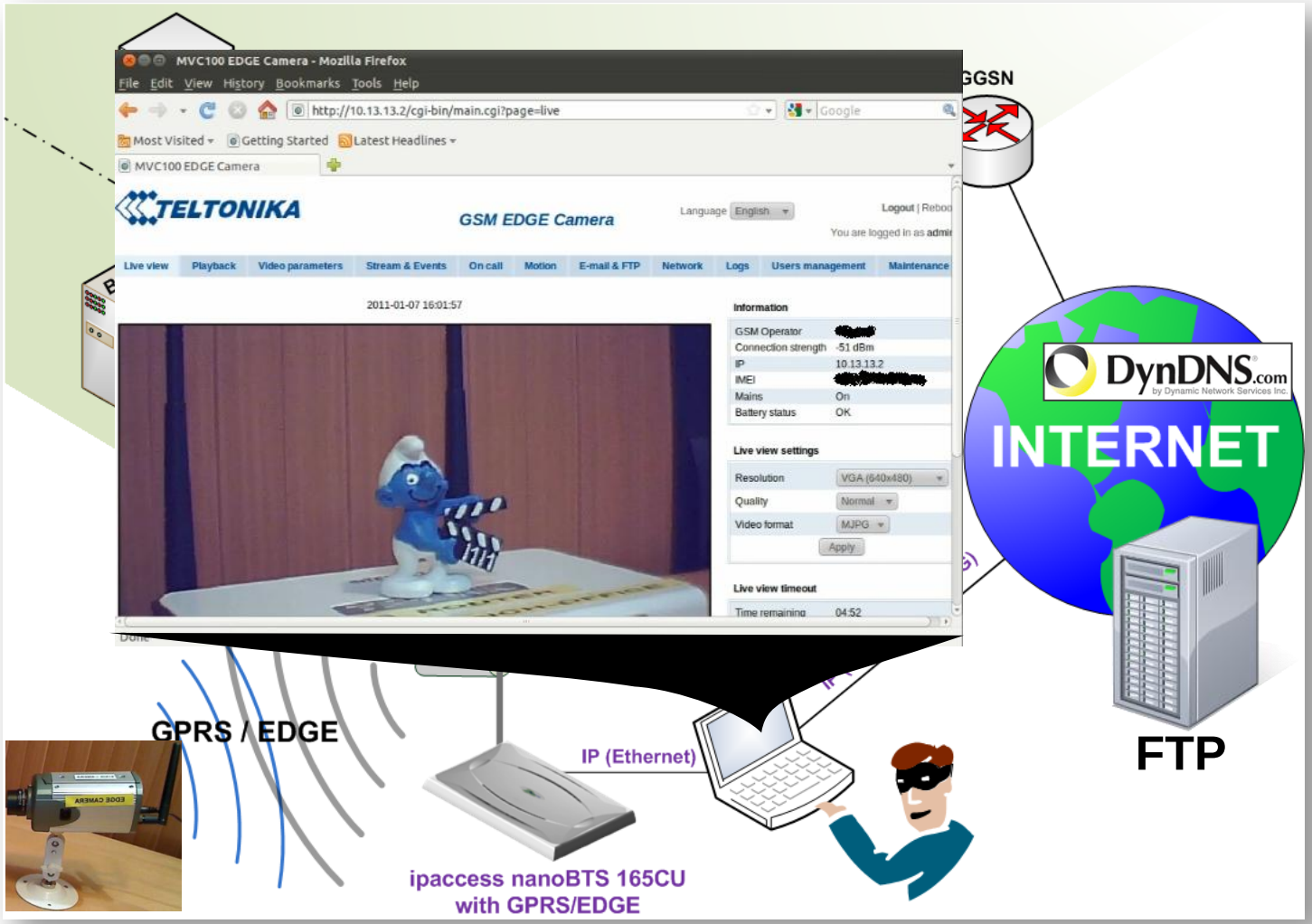
¿Qué ha sucedido?



Aprovechando el ataque: ejemplo 5

Ataques contras otro dispositivos GPRS/EDGE

¿Qué ha sucedido?



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