



# ¿Son seguras las comunicaciones móviles?

David Pérez  
José Picó

Cádiz, 25 de Febrero de 2011



- Introducción
- Vectores de ataque
- Ataques contra GSM
- Ataques contra GPRS/EDGE
- Extensión a UMTS
- Contramedidas



---

# Introducción

---

# Dispositivos móviles como fuente de amenaza



- Cada vez más, los dispositivos móviles tienen acceso a información sensible
  - Correo electrónico
  - Acceso a servicios “cloud”
  - Aplicaciones corporativas
- Son ya una de las vías de ataque en proceso de investigación

# Dispositivos móviles como fuente de amenaza



- Teléfono móvil = un ordenador portátil de su empresa:
  - sistema operativo que es una variación de un estándar
  - conexión a internet (vía Wifi ó 3G)
  - acceso a datos internos (correo, documentación).

# Dispositivos móviles como fuente de amenaza



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



---

# Vectores de ataque

---

# Comunicaciones móviles expuestas a varios vectores



**Vulnerabilidades del protocolo**



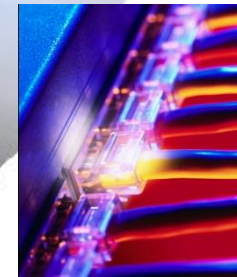
**Ataques criptográficos**



**Ataques OTA**



**Corrupción de memoria**



**Desde el operador**

# Debilidades de GSM (I)



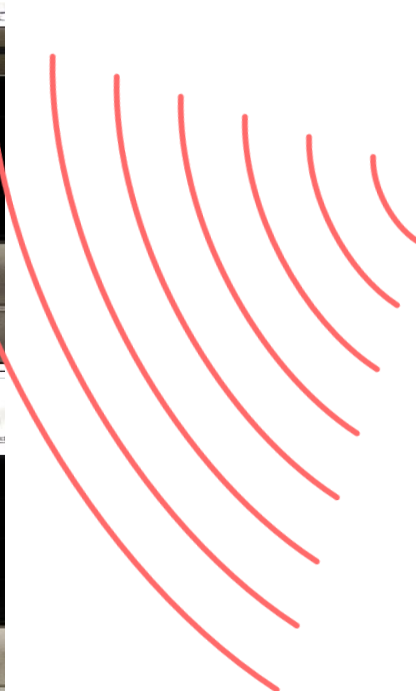
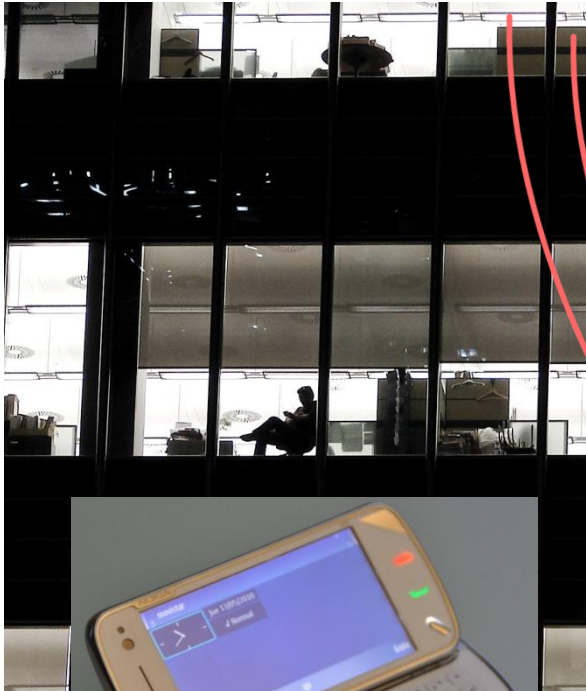
- El IMSI, que es una información sensible porque revela si determinado usuario está en una ubicación, se envía en claro en numerosas ocasiones y puede forzarse a ser enviado mediante ataques activos
- La norma refiere la necesidad de soportar A5/0 como método de cifrado
- Debilidades de los algoritmos de cifrado A5
  - Padding y corrección de errores antes del cifrado
  - Otras debilidades criptológicas

# Debilidades de GSM (II)



- No existe autenticación inversa, es decir de la red contra la MS, lo que posibilita la suplantación de la red
- La obtención de  $K_c$  sólo depende de RAND y  $K_i$  por lo que, si de alguna forma un atacante logra conseguir el  $K_c$  que corresponde a un determinado RAND para esa MS, puede descifrar una conversación grabada con anterioridad con ese mismo RAND o con esa misma  $K_c$

# Ataque mediante estación base falsa



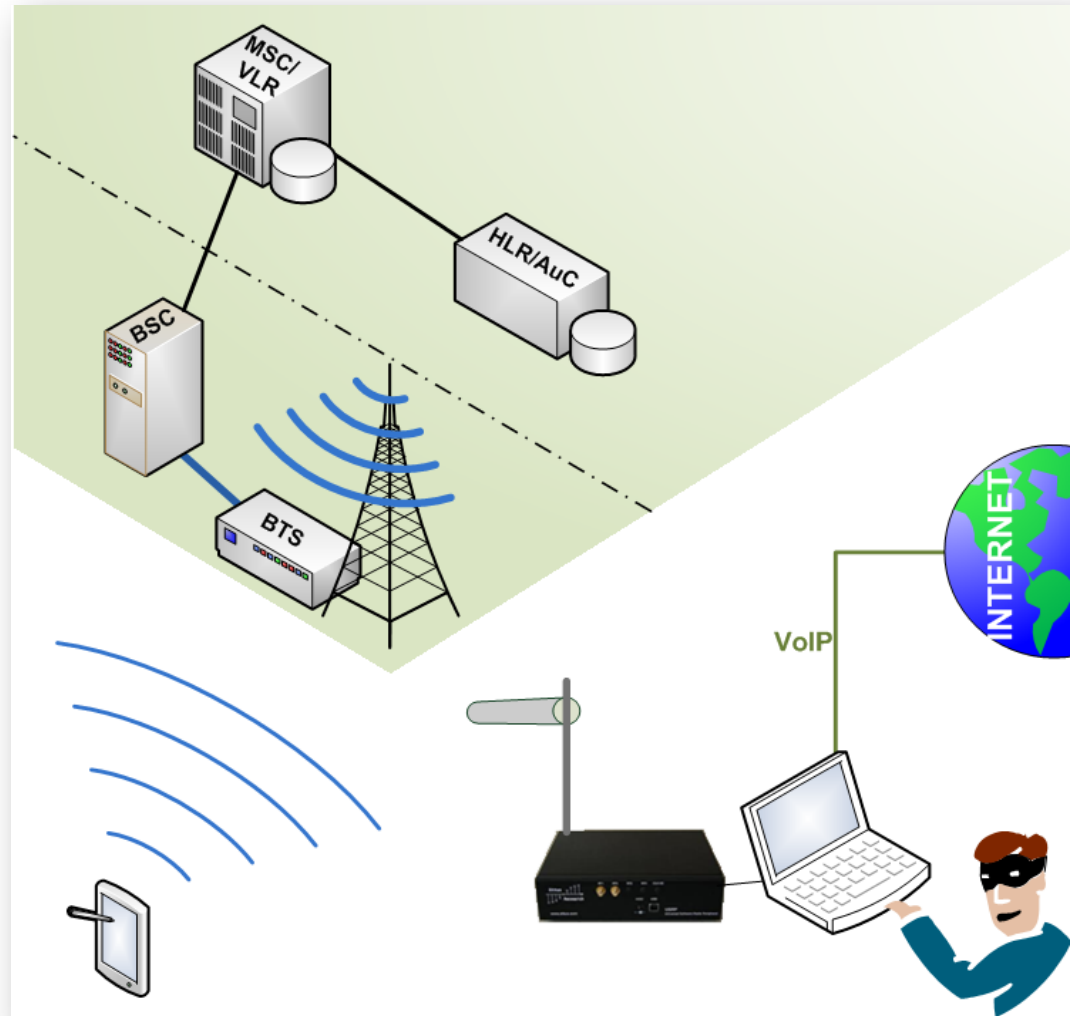
movistar



# Ataque: fase inicial



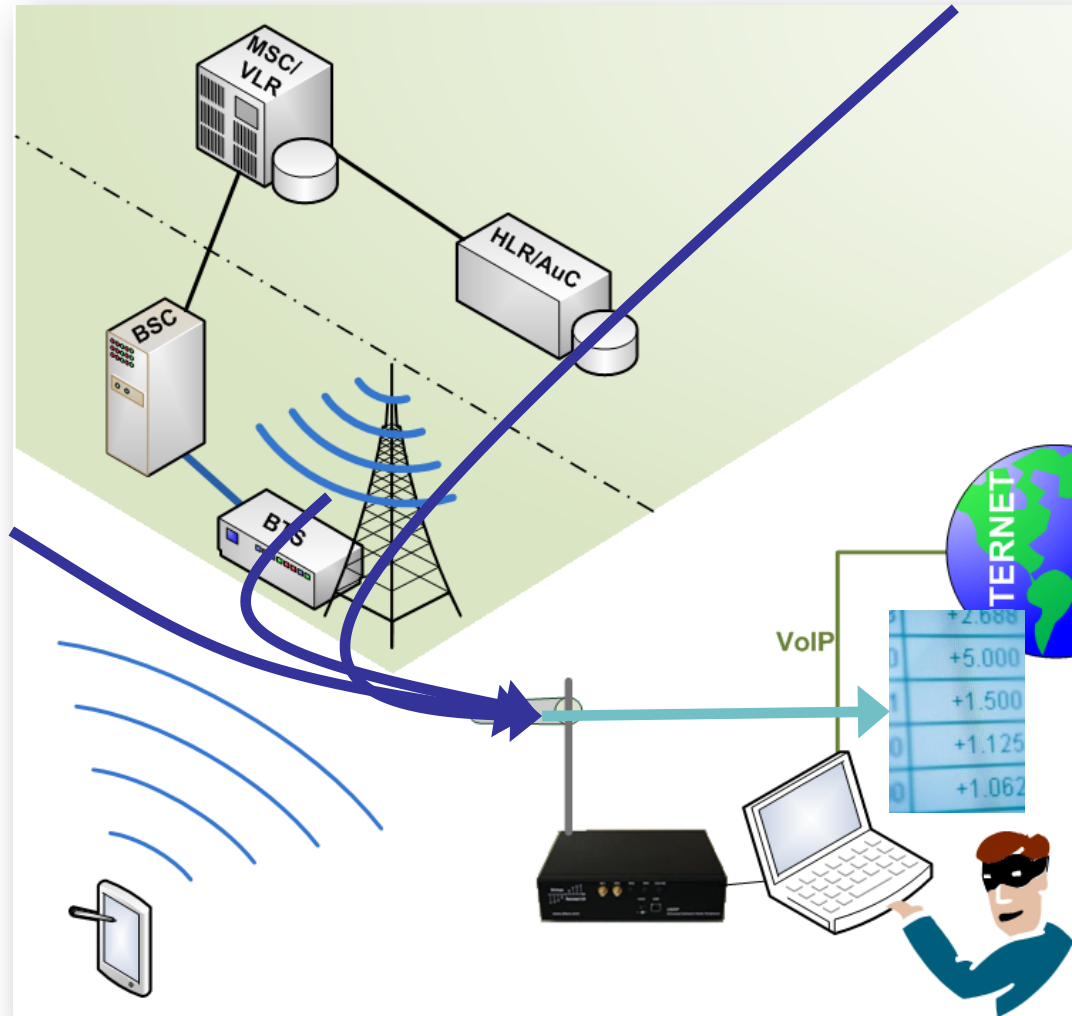
Ubicación de la infraestructura



# Ataque: paso 1



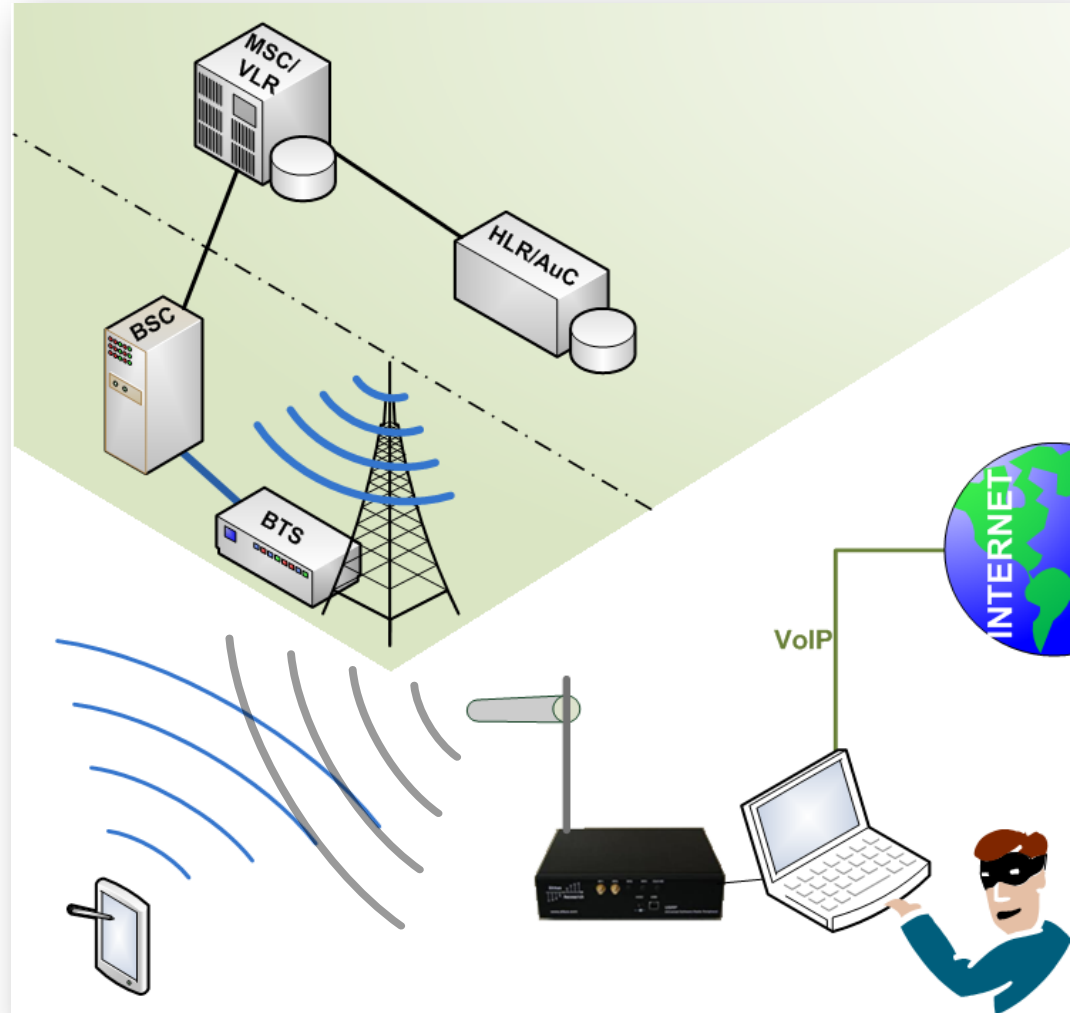
Caracterización de la celda



# Ataque: paso 2



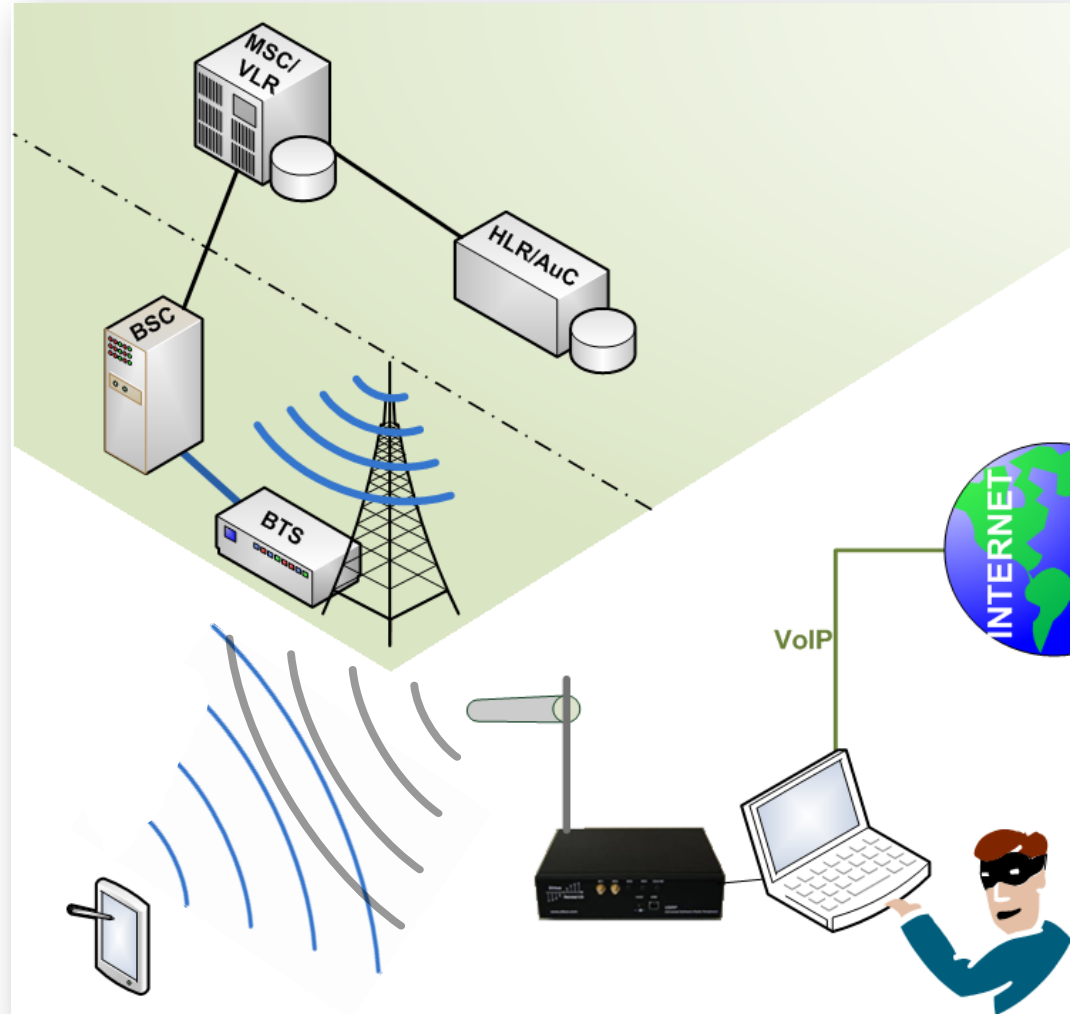
El atacante comienza a emitir



# Ataque: paso 3



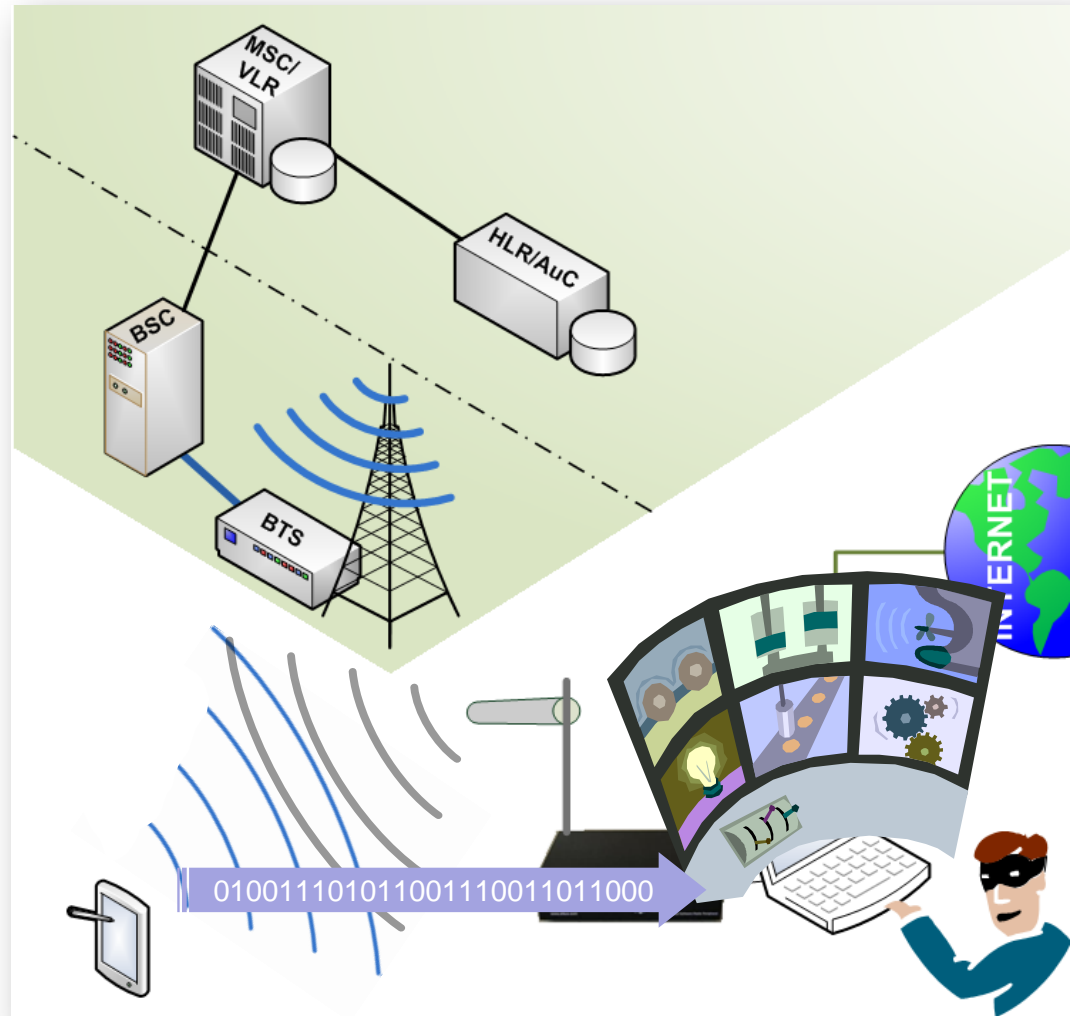
La víctima campa en la celda falsa



# Ataque: paso 4



El atacante toma control total de las comunicaciones de voz de la víctima





---

# Ataques contra GSM

---



Si el teléfono suena, pero no lo cogen, es que no están

¿Seguro?



Nuestra conversación es privada.

¿Seguro?



# Nuestros SMS son privados.

¿Seguro?



Los SMS que recibimos son legítimos.

¿Seguro?



# Sabemos quién nos llama.

¿Seguro?



# Sabemos a quién llamamos.

¿Seguro?



Sabemos a quién llamamos...

*...reloaded*

¿Seguro?



---

# Ejemplos de uso del ataque contra GPRS/EDGE

---



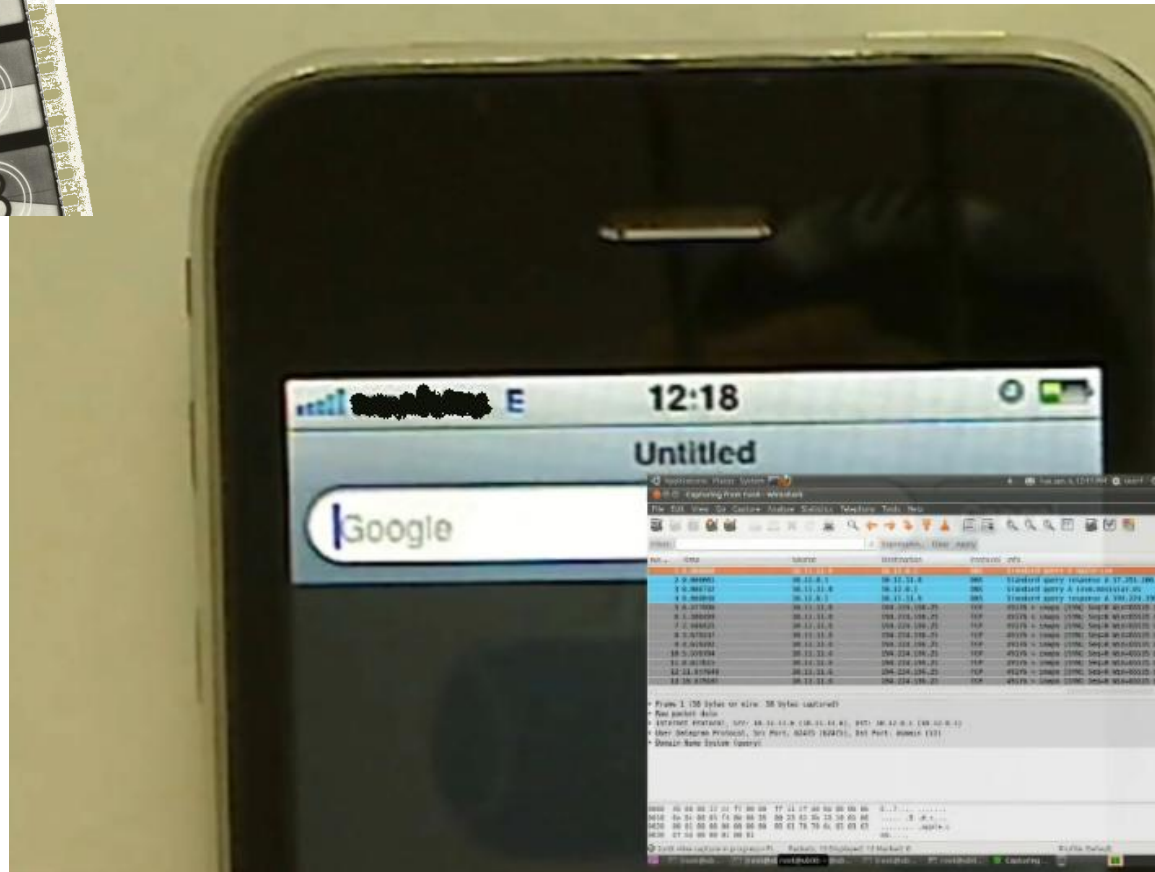
- Autenticación unidireccional
- Soporte a GEA0 (no cifrado)
- Soporte a degradación  
UMTS→GPRS/EDGE

Igual que GSM

# Aprovechando el ataque: ejemplo 1



Un atacante escucha el tráfico de una búsqueda realizada con un iPhone



# ¿Qué ha pasado?



**Capturing from tun0 - Wireshark**

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 W...
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 W...
414	59.479399	10.11.11.6	194.224.196.25	TCP	49190 > imap[s] [SYN] Seq=0 Win=65535 Le...
415	60.518596	10.11.11.6	194.224.196.25	TCP	49190 > imap[s] [SYN] Seq=0 Win=65535 Le...
416	61.847016	10.11.11.6	194.224.196.25	TCP	49190 > imap[s] [SYN] Seq=0 Win=65535 Le...
417	62.779089	10.11.11.6	194.224.196.25	TCP	49190 > imap[s] [SYN] Seq=0 Win=65535 Le...
418	63.697499	10.11.11.6	194.224.196.25	TCP	49190 > imap[s] [SYN] Seq=0 Win=65535 Le...
419	66.778060	10.11.11.6	194.224.196.25	TCP	49190 > imap[s] [SYN] Seq=0 Win=65535 Le...
420	69.833199	10.11.11.6	194.224.196.25	TCP	49190 > imap[s] [SYN] Seq=0 Win=65535 Le...
421	77.888696	10.11.11.6	194.224.196.25	TCP	49190 > imap[s] [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 00 .....5.#+...  
0020 00 01 00 00 00 00 00 00 05 61 70 70 6c 65 03 63 .....apple.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**

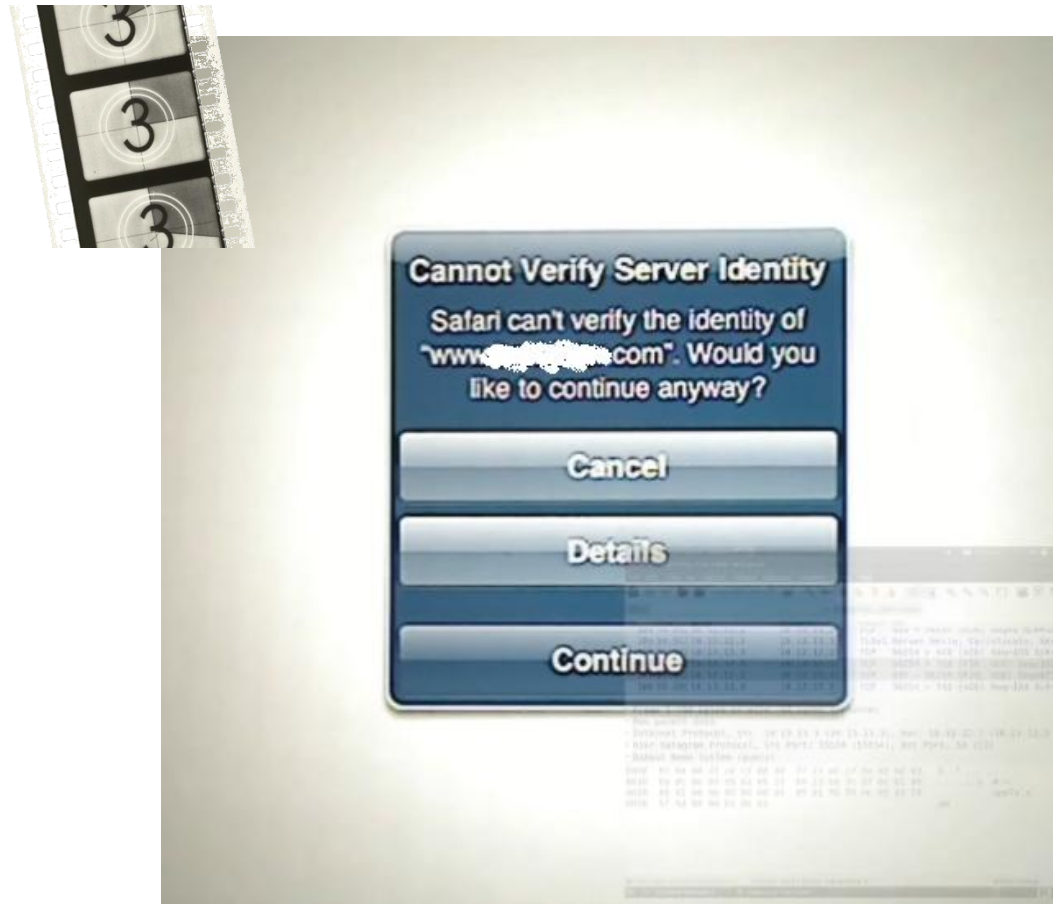
**INTERNET**

**GGSN**

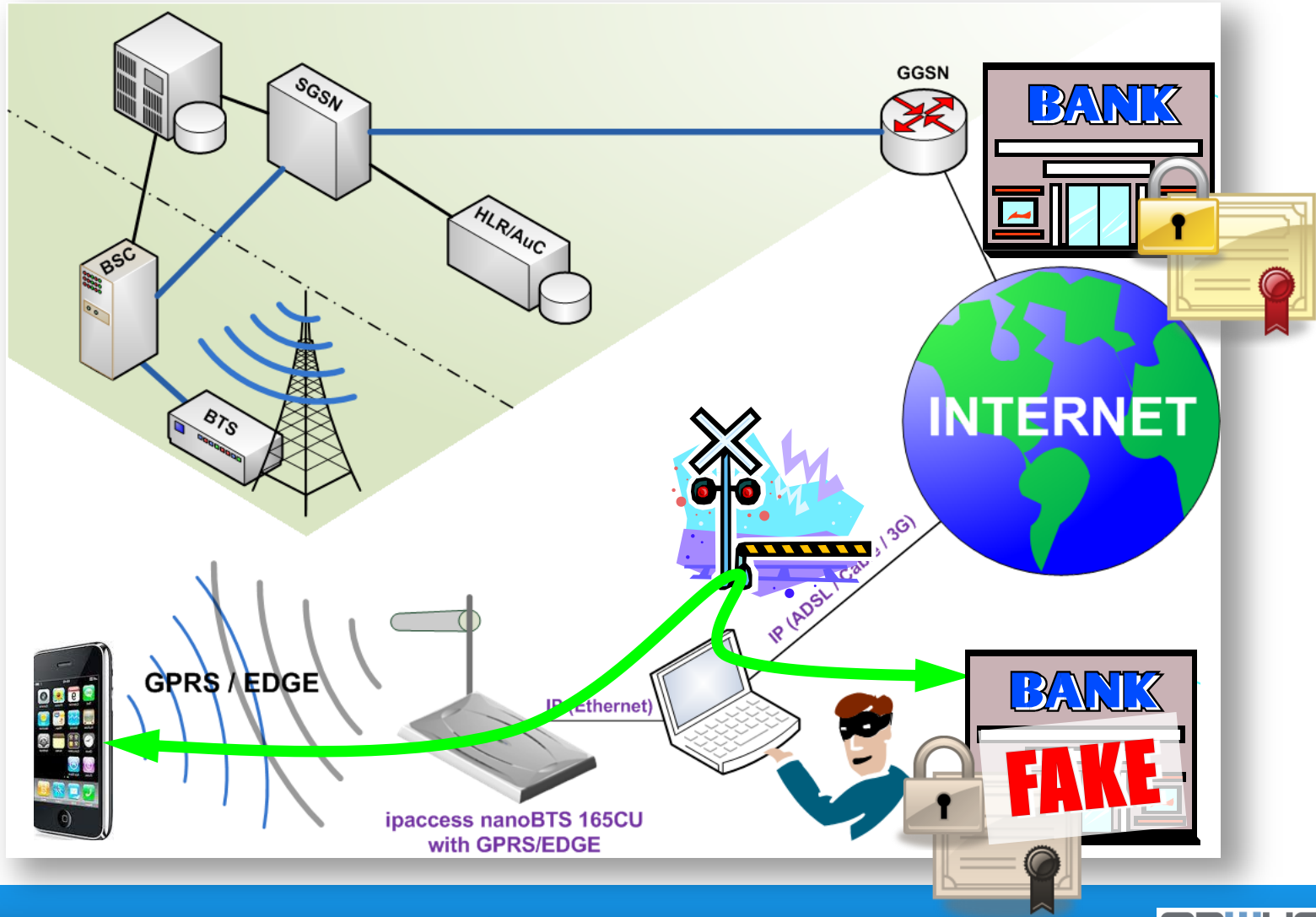
# Aprovechando el ataque: ejemplo 2



## Phishing attack against an iPad (https version)



# ¿Qué ha pasado?





---

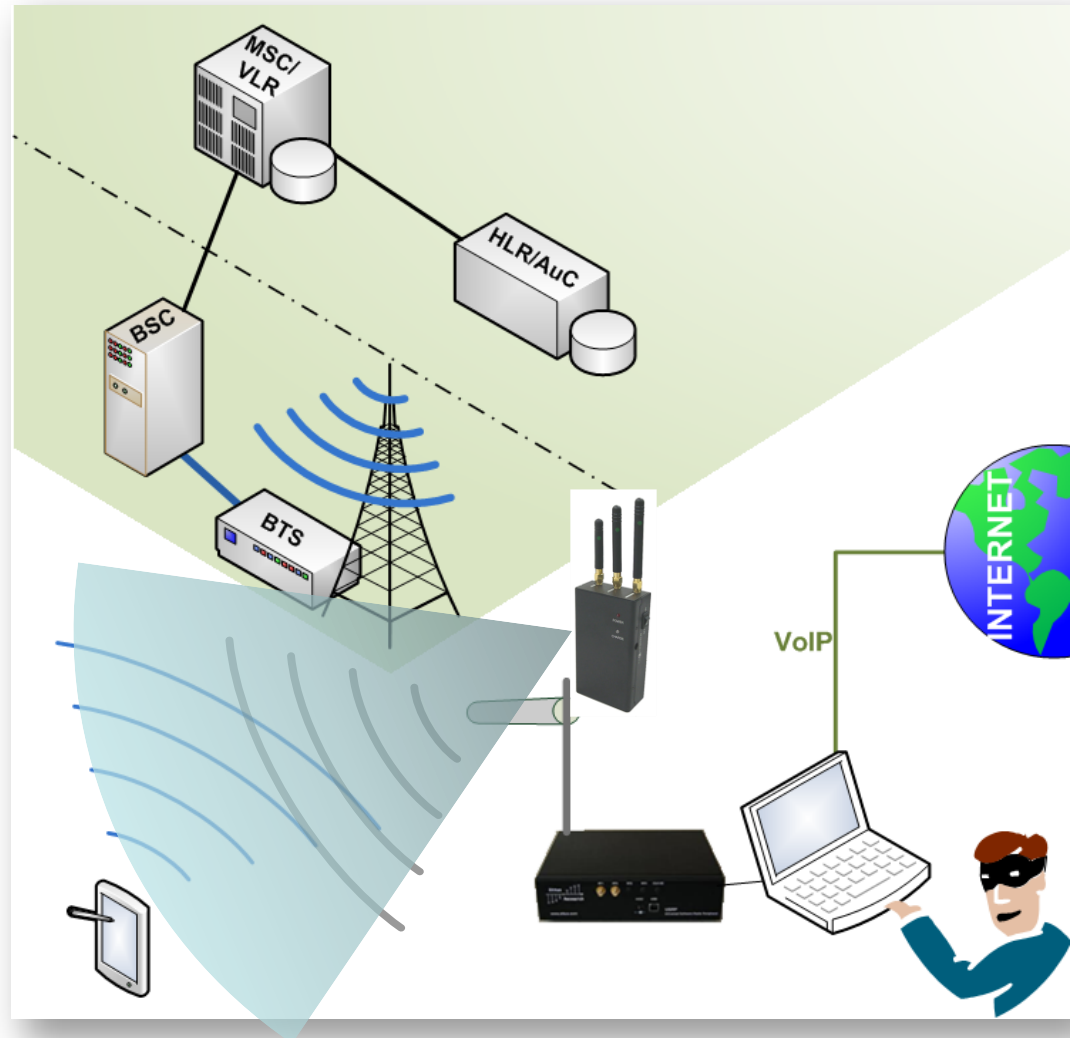
# Extensión a UMTS

---

# Extensión a UMTS: simplemente se añade el paso 0



Interferir la banda  
UMTS





---

# Contramedidas

---

# ¿Qué se puede hacer?



- Configurar nuestros dispositivos móviles para que sólo acepten servicio 2G
- Cifrar nuestras comunicaciones a niveles superiores (cifrado de voz, https, ssh, IPsec, etc.)
- SW adicional de detección de situaciones “anómalas”
- Instalar y configurar firewall en el móvil (GPRS/EDGE)



# ¿Son seguras las comunicaciones móviles?

David Pérez – [david@taddong.com](mailto:david@taddong.com)

José Picó – [jose@taddong.com](mailto:jose@taddong.com)