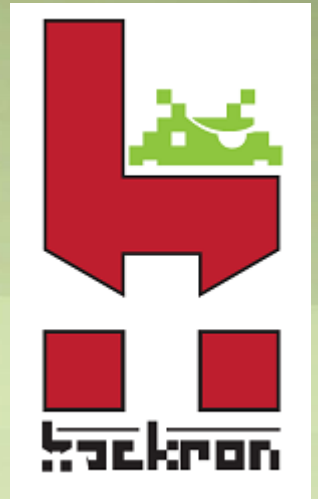




www.layakk.com

@layakk



3G Attacks

José Picó García
(David Pérez Conde)



Agenda

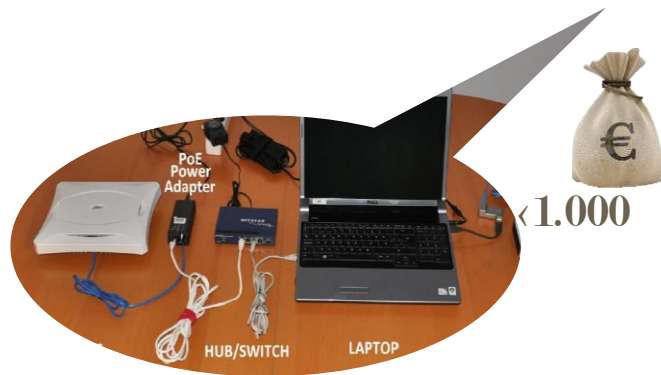
- ▶ Introducción
- ▶ El problema de la configuración de la celda falsa
- ▶ IMSI Catching
- ▶ Denegación de servicio
- ▶ Trabajos en marcha y futuros
- ▶ Conclusiones

Introducción

y un poco de historia...



Las comunicaciones móviles 2G son totalmente vulnerables



(*) **NOTA:** solamente teniendo en cuenta los ataques con estación base falsa

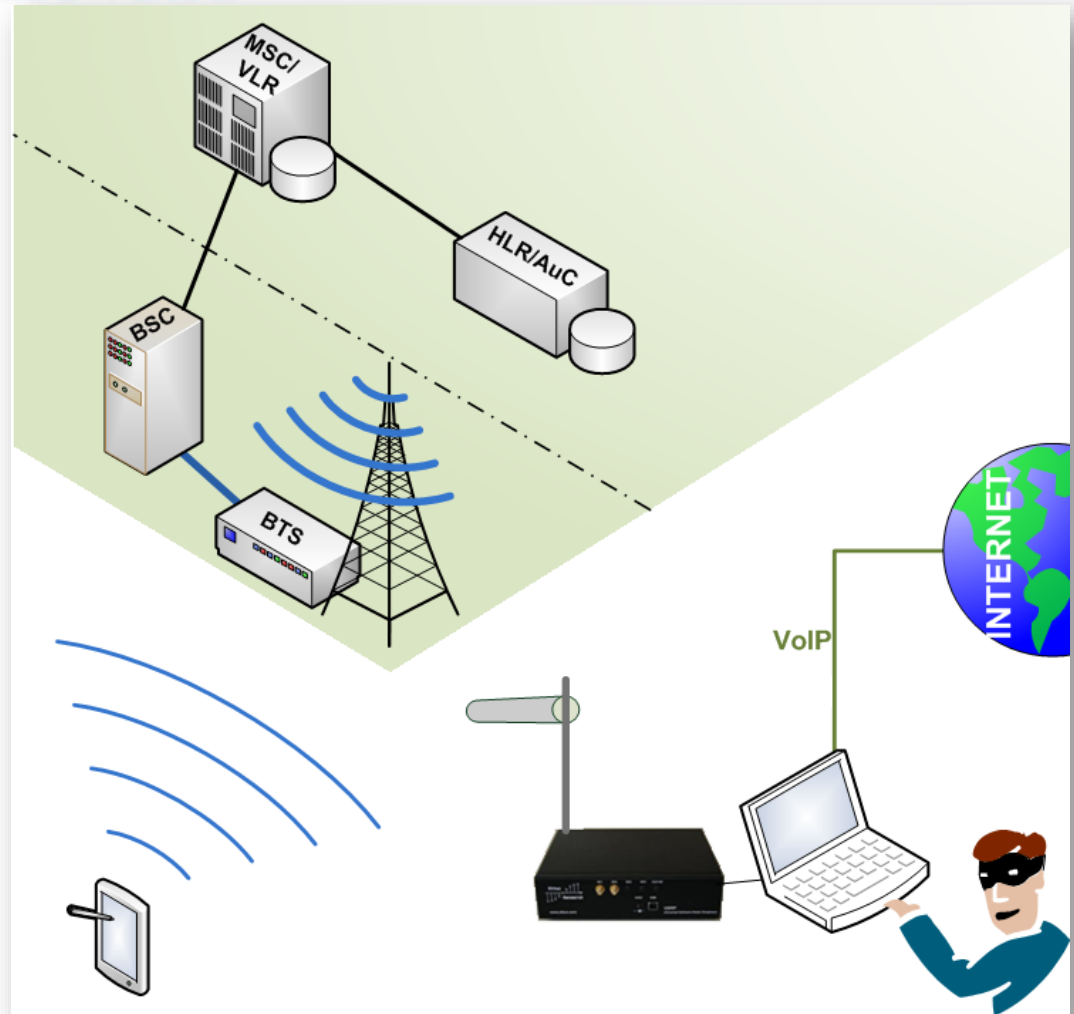
- >Interceptación
- >Manipulación
- >Identificación de usuarios
- >Geolocalización
- >Denegación de servicio



Las comunicaciones móviles 2G son totalmente vulnerables

Ataque con estación base falsa

→ Ubicación de la infraestructura

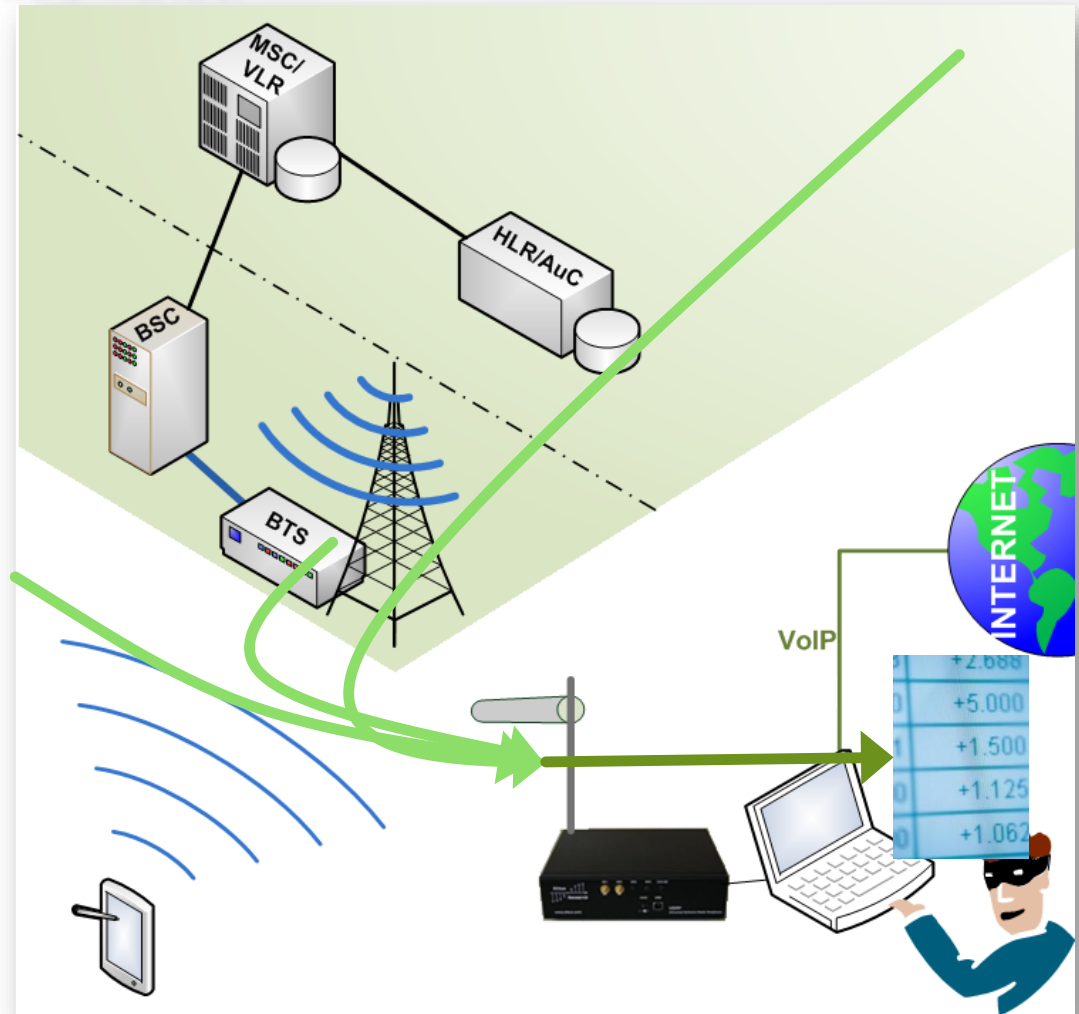




Las comunicaciones móviles 2G son totalmente vulnerables

Ataque con estación base falsa

→ Caracterización de la celda

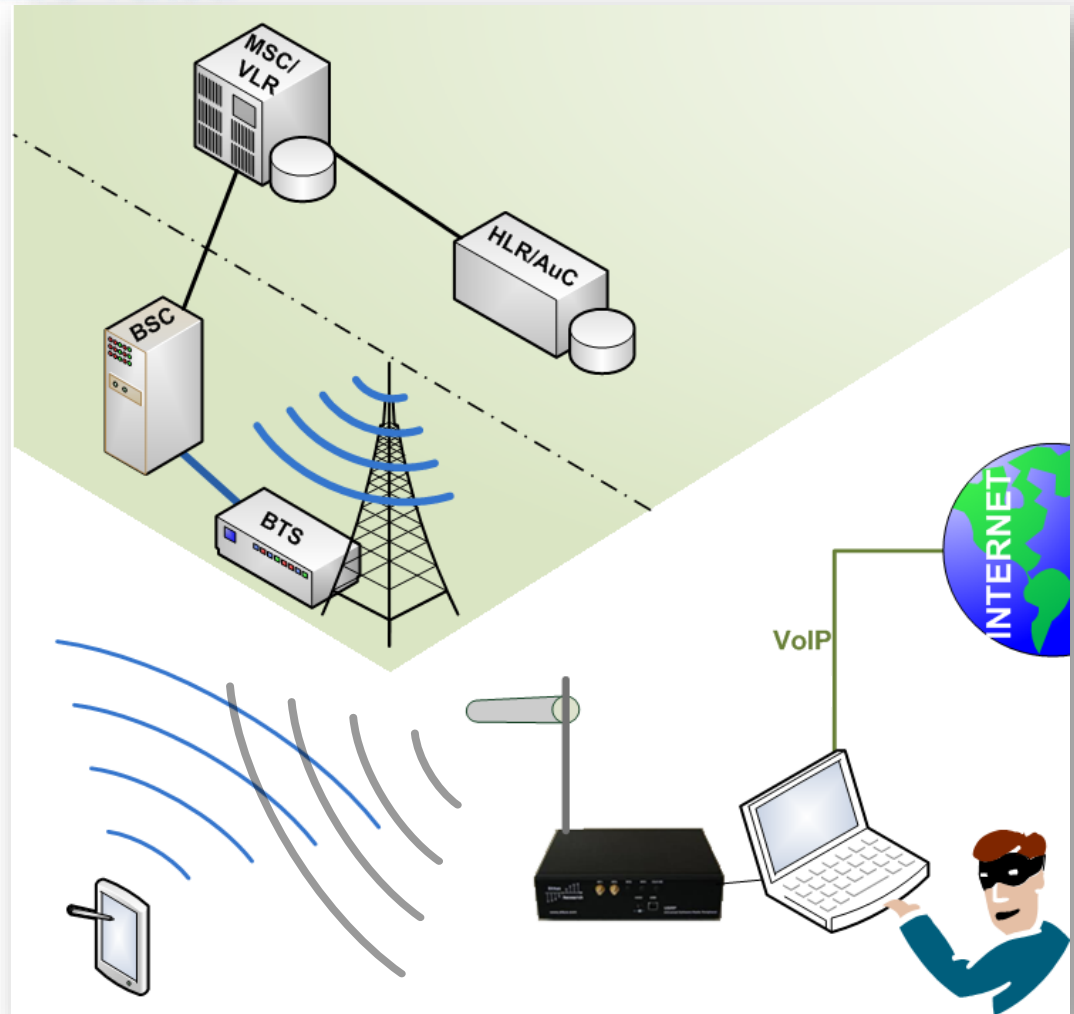




Las comunicaciones móviles 2G son totalmente vulnerables

Ataque con estación base falsa

→ Atacante comienza a emitir

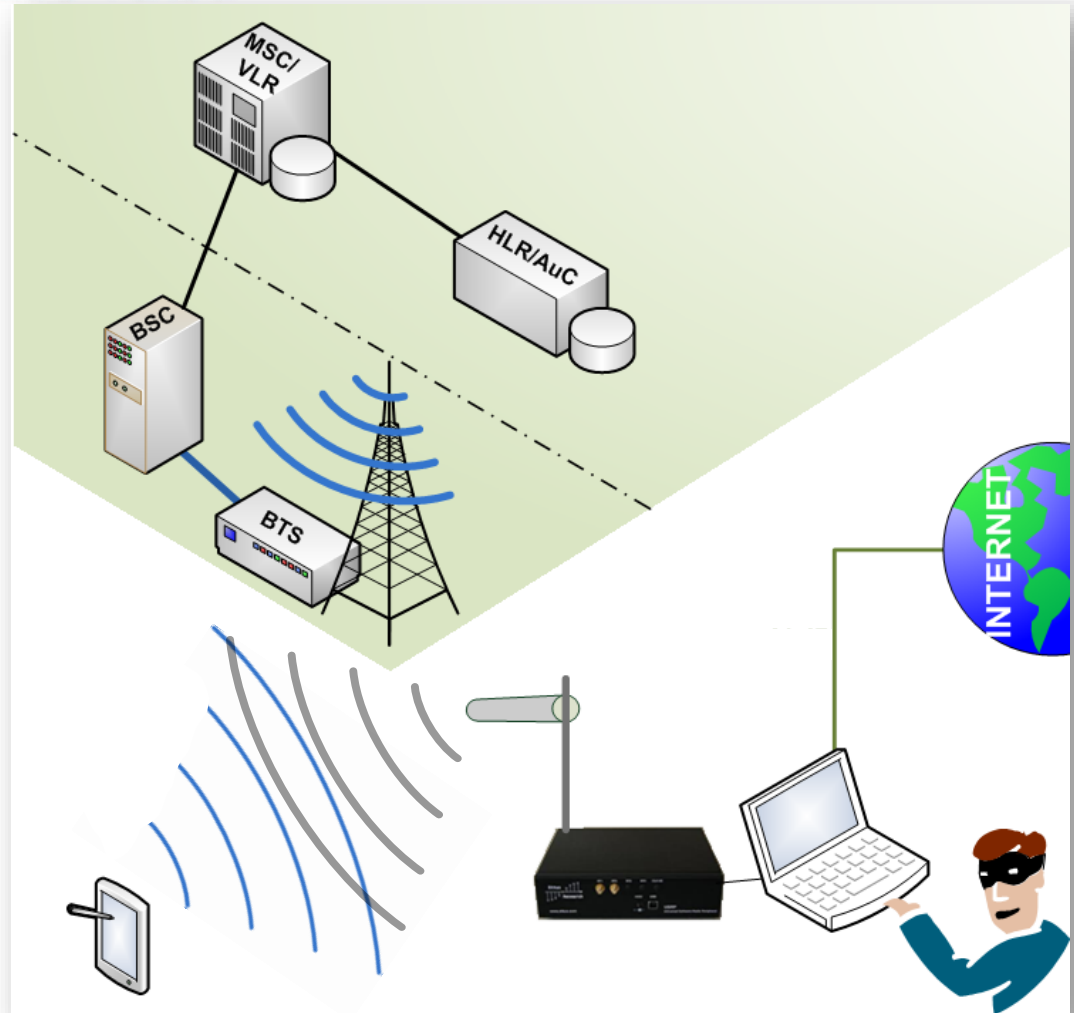




Las comunicaciones móviles 2G son totalmente vulnerables

Ataque con estación base falsa

→ La víctima cae en la celda falsa

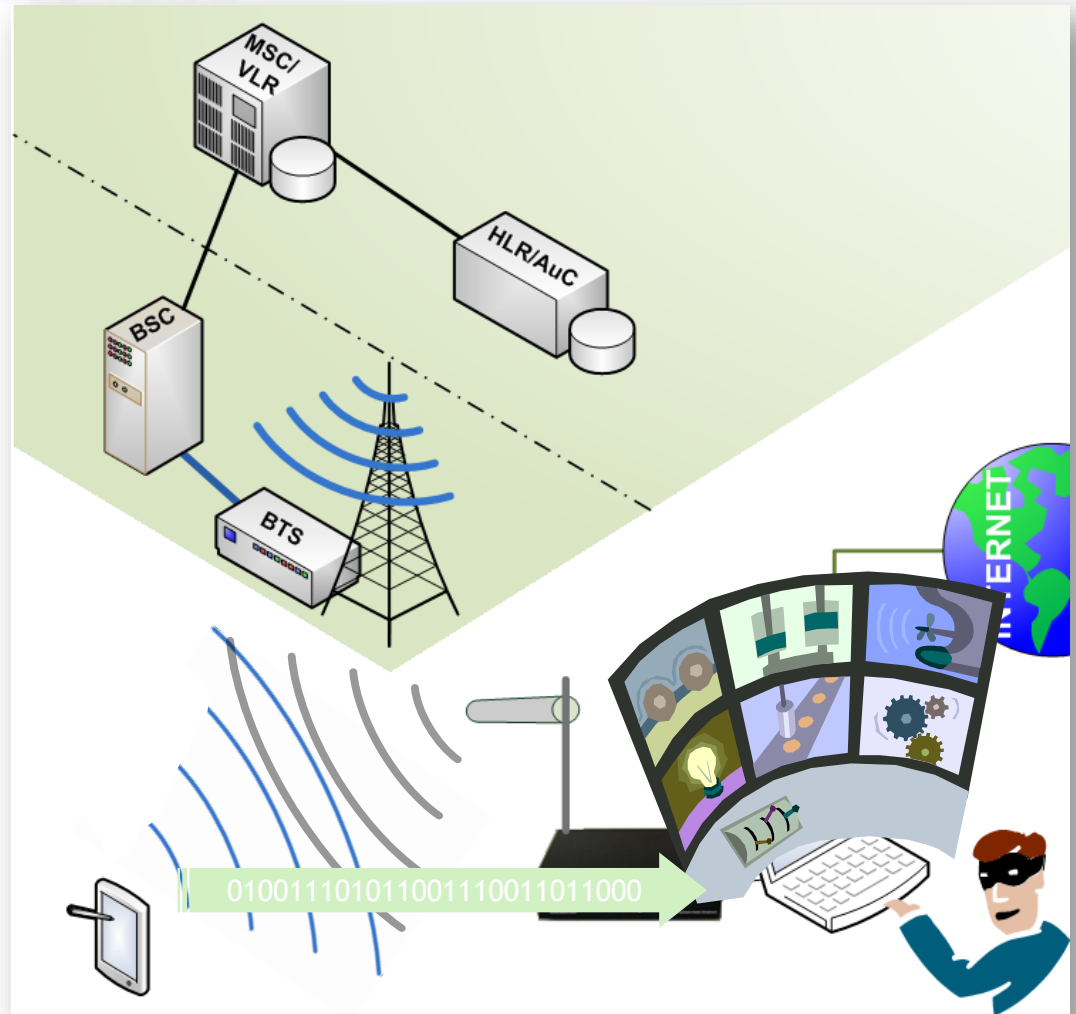




Las comunicaciones móviles 2G son totalmente vulnerables

Ataque con estación base falsa

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





Las comunicaciones móviles 2G son totalmente vulnerables

En la práctica...



>Interceptación

>Manipulación

>Identificación de usuarios

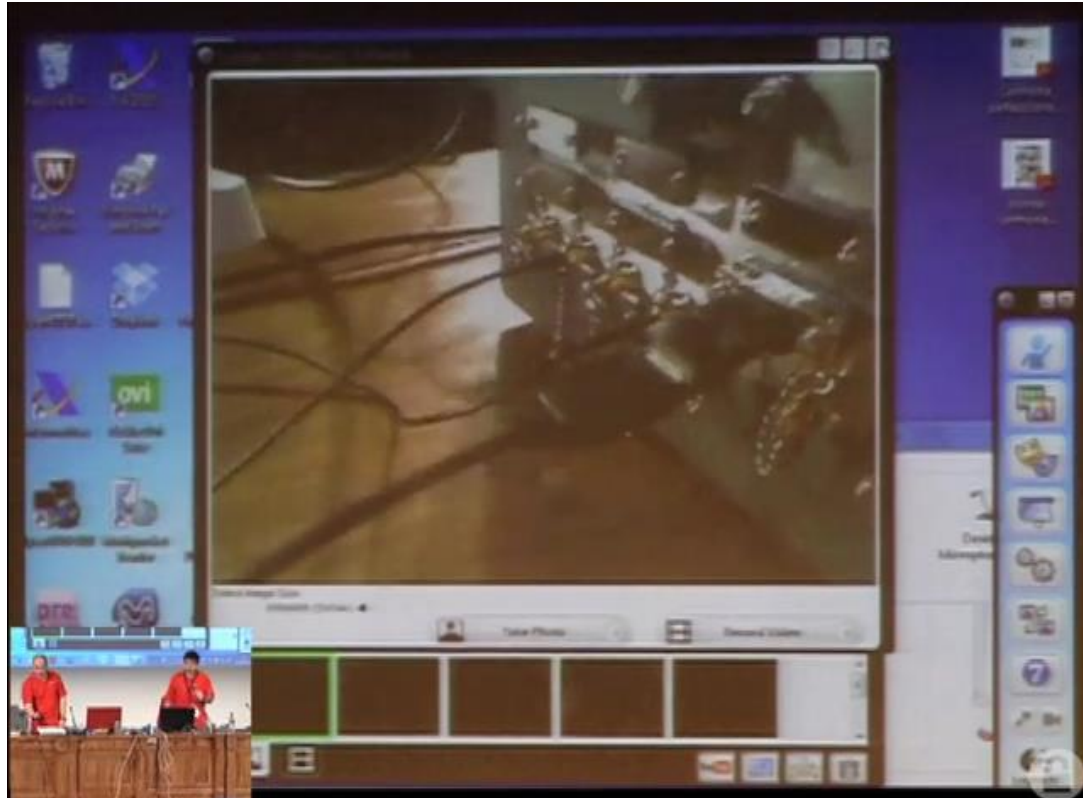
>Geolocalización

>Denegación de servicio



Las comunicaciones móviles 2G son totalmente vulnerables

En la práctica...



>Interceptación

>**Manipulación**

>Identificación
de usuarios

>Geolocalización

>Denegación de
servicio



Las comunicaciones móviles 2G son totalmente vulnerables

En la práctica...

```
root@port2-laptop: /tmp
1273093890.3109 INFO 3067259760 GSML3Message.cpp:162:parseL3: L3 recv MM Location
Updating Request LAI=(MCC=214 MNC=07 LAC=0xffff) MobileIdentity=(IMSI=214070000000000)
1273093890.3110 INFO 3067259760 MobilityManagement.cpp:139:LocationUpdatingContr
oller: MM Location Updating Request LAI=(MCC=214 MNC=07 LAC=0xffff) MobileIdenti
ty=(IMSI=214070000000000)
1273093890.3111 INFO 3067259760 SIPEngine.cpp:148:Register: SIPEngine::Register
mState=NULL 0 callID 1430490275
1273093890.3111 INFO 3067259760 SIPInterface.cpp:107:addCall: creating SIP messa
ge FIFO callID 1430490275
1273093890.3115 INFO 3067259760 SIPInterface.cpp:167:write: write REGISTER sip:1
27.0.0.1 SIP/2.0
1273093890.3805 INFO 3069922160 SIPInterface.cpp:192:drive: read SIP/2.0 200 OK
1273093890.3808 INFO 3067259760 SIPInterface.cpp:114:removeCall: removing SIP me
ssage FIFO callID 1430490275
1273093890.3810 INFO 3067259760 MobilityManagement.cpp:189:LocationUpdatingContr
oller: registration SUCCESS: IMSI=214070000000000
1273093890.3810 INFO 3067259760 GSMLLogicalChannel.cpp:76:send: L3 SAP0 sending M
M MM Information short name=(movistar?)
1273093890.3812 INFO 3067259760 GSMLLogicalChannel.cpp:76:send: L3 SAP0 sending M
M Location Updating Accept LAI=(MCC=214 MNC=07 LAC=0x29a) ID=(TMSI=0x4beldedd)
1273093890.7825 INFO 3067259760 MobilityManagement.cpp:119:sendWelcomeMessage: s
ending Control.NormalRegistrationWelcomeMessage message to handset
```

>Interceptación

>Manipulación

>Identificación
de usuarios

>Geolocalización

>Denegación de
servicio



Las comunicaciones móviles 2G son totalmente vulnerables

En la práctica...

Building a distance estimation model based on time measurements

After Phase 1 of adjustments

- Precision was not enough yet ☹
- Figure: where do these circles intersect?



BRUCON
SECURITY TRAINING
GHENT 23 - 24 - 25
SEPTEMBER
2- or 3-day courses
by renowned experts



BRUCON
SECURITY CONFERENCE
GHENT 26 - 27 SEPTEMBER
2-day conference
featuring outstanding security
presentations and workshops



>Interceptación

>Manipulación

>Identificación de usuarios

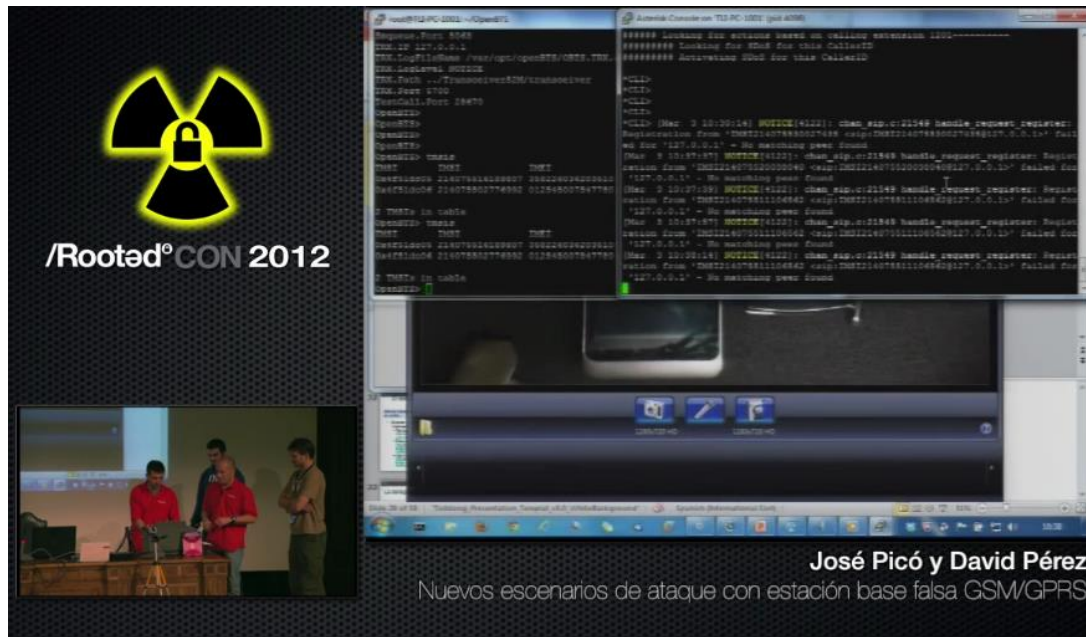
>**Geolocalización**

>Denegación de servicio



Las comunicaciones móviles 2G son totalmente vulnerables

En la práctica...

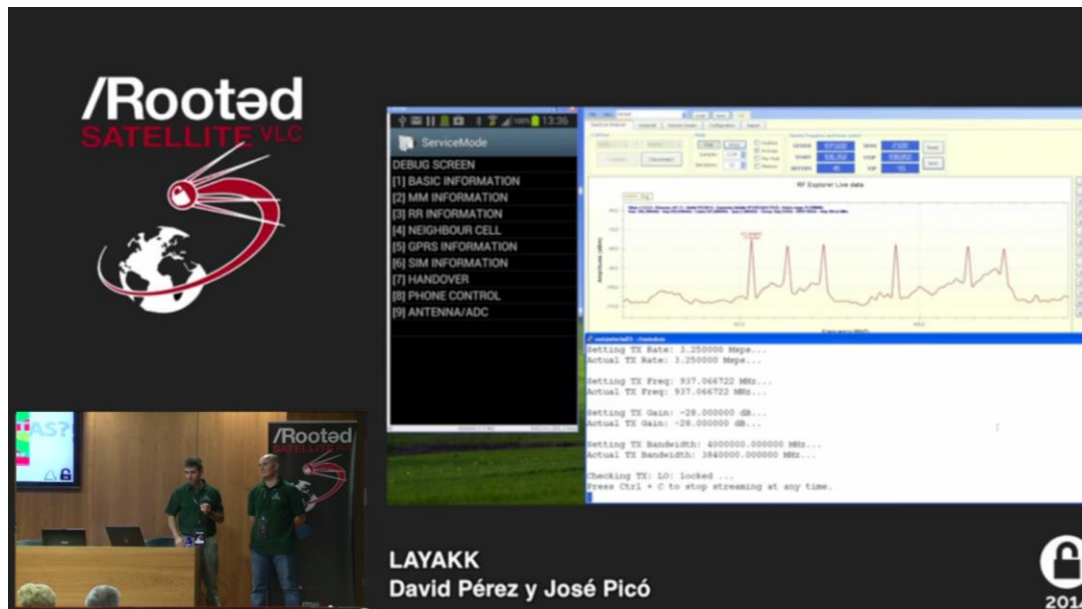


- >Interceptación
- >Manipulación
- >Identificación de usuarios
- >Geolocalización
- >Denegación de servicio



Las comunicaciones móviles 2G son totalmente vulnerables

En la práctica...



>Interceptación

>Manipulación

>Identificación de usuarios

>Geolocalización

>Denegación de servicio



¿Es posible aplicar estas técnicas a 3G?

- ▶ En 3G existe autenticación bidireccional
- ▶ La criptografía de 3G no está rota públicamente
- ▶ sin embargo...



En 2014 ya pensábamos que una parte de los ataques era posible...

/Rooted® 2014

Conclusiones

creemos que

- Ataques posibles en **3G** utilizando la técnica de estación base falsa:
 - IMSI Catching
 - Geolocalización de dispositivos
 - Denegación de servicio
 - Interceptación de comunicaciones
 - *Downgrade selectivo a 2G*
- En 3G existen dispositivos comerciales que cubren parte de la funcionalidad anterior
- Algunos investigadores "de renombre" dicen que en 3G ~~no~~ se pueden realizar estos ataques... *creemos que*
- ... en esta charla os contamos que gran parte de lo anterior sí puede hacerse...
- ... pero sobre todo queremos ¿desvelar? cómo.



Base teórica

/Rooted® 2014

¿Cómo es posible?

- Los mensajes de señalización en 3G están protegidos en integridad, gracias al *security mode command* y a la estructura del protocolo
- La criptografía después de la protección de integridad y del cifrado no ha sido rota (al menos públicamente).

¿Todos los mensajes?



Rooted COH 2014 6-7-8 Marzo // 6-7-8 March.

/Rooted® 2014

Mensajes de señalización RRC no protegidos en integridad

- HANDOVER TO UTRAN COMPLETE
- PAGING TYPE 1
- PUSCH CAPACITY REQUEST
- PHYSICAL SHARED CHANNEL ALLOCATION
- SYSTEM INFORMATION
- SYSTEM INFORMATION CHANGE INDICATION
- TRANSPORT FORMAT COMBINATION CONTROL (TM DCCH only)

- RRC CONNECTION REQUEST
- RRC CONNECTION SETUP
- RRC CONNECTION SETUP COMPLETE
- RRC CONNECTION REJECT
- RRC CONNECTION RELEASE (CCCH only)



Rooted COH 2014 6-7-8 Marzo // 6-7-8 March

/Rooted® 2014

Mensajes MM (DL) permitidos antes del security mode command

- AUTHENTICATION REQUEST
- AUTHENTICATION REJECT
- IDENTITY REQUEST
- LOCATION UPDATING REJECT
- LOCATION UPDATING ACCEPT (at periodic location update with no change of location area or temporary identity)
- CM SERVICE ACCEPT, if the following two conditions apply:
 - no other MM connection is established; and
 - the CM SERVICE ACCEPT is the response to a CM SERVICE REQUEST with CM SERVICE TYPE IE set to 'emergency call establishment'
- CM SERVICE REJECT
- ABORT



Rooted COH 2014 6-7-8 Marzo // 6-7-8 March

El problema de la configuración y parametrización de la celda falsa

¿Quién vive en el vecindario?



Las celdas vecinas





- [illegible]

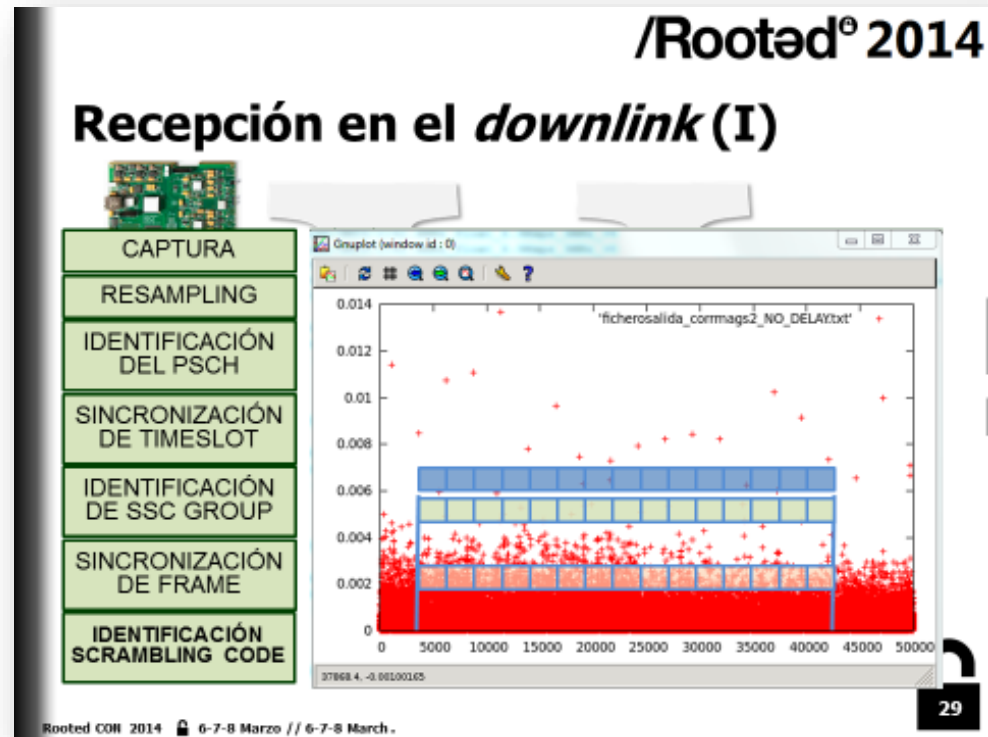
21



Solución Ideal

- Un sniffer de 3G, DL y UL, de los mensajes de control (Broadcast y algunos dedicados)

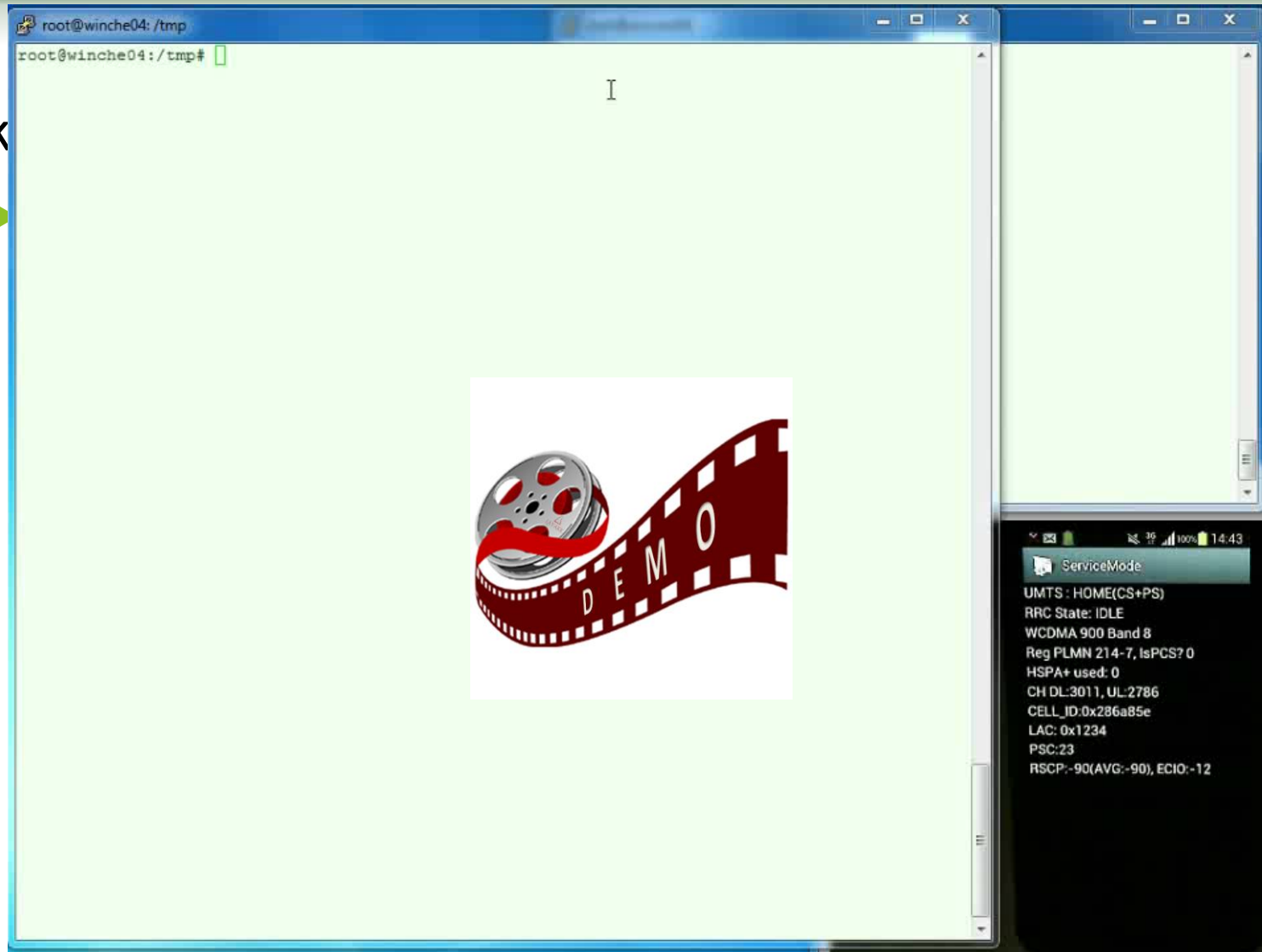
→ *En progreso*





Solución alternativa

► lk

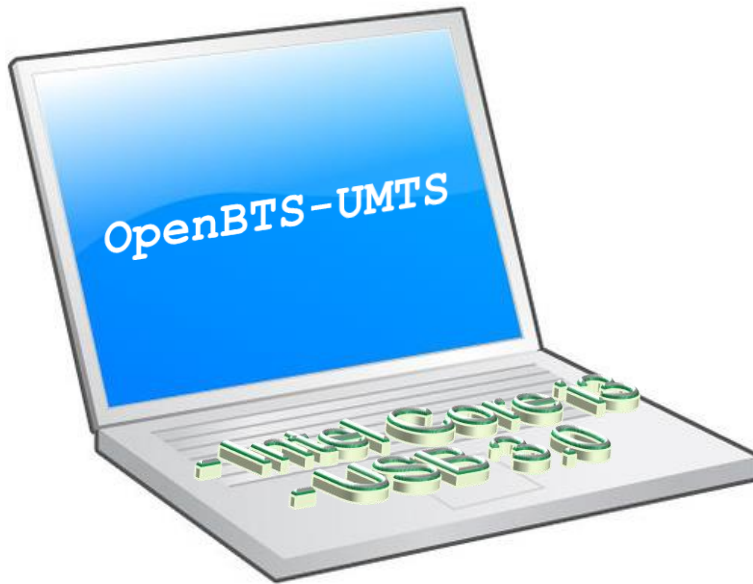


Infraestructura estación base 3G

¿Qué hace falta?



Lo que nosotros utilizamos...



Ref.: OpenBTS-UMTS

<http://openbts.org/w/index.php/OpenBTS-UMTS>

Ref.: USRP B200

<http://www.ettus.com/product/details/UB200-KIT>



Lo que nosotros utilizamos...



IMSI Catching

¿En qué consiste?

¿Por qué es peligroso?

Pruebas en 3G



IMSI Catching

¿Qué es el IMSI?

- ▶ El IMSI (Internation Mobile Subscriber Number) es el número que identifica a los usuarios de la red móvil

MCC	MNC	MSIN
-----	-----	------

- ▶ Está asociado a cada SIM y, por extensión, a la persona que lo compra
- ▶ Es el único identificador de usuario (en el nivel de movilidad de la comunicaciones móviles) que es invariable
- ▶ Sólo debe ser conocido por el operador y por el usuario



IMSI Catching

¿En qué consiste?

- ▶ Consiste en la captura no autorizada de IMSIs
- ▶ Puede hacerse utilizando diferentes técnicas
 - ▶ la que nos ocupa es la utilización de una estación base falsa
 - ▶ en este caso, la captura se hace en el entorno del atacante

¿Por qué es peligroso?

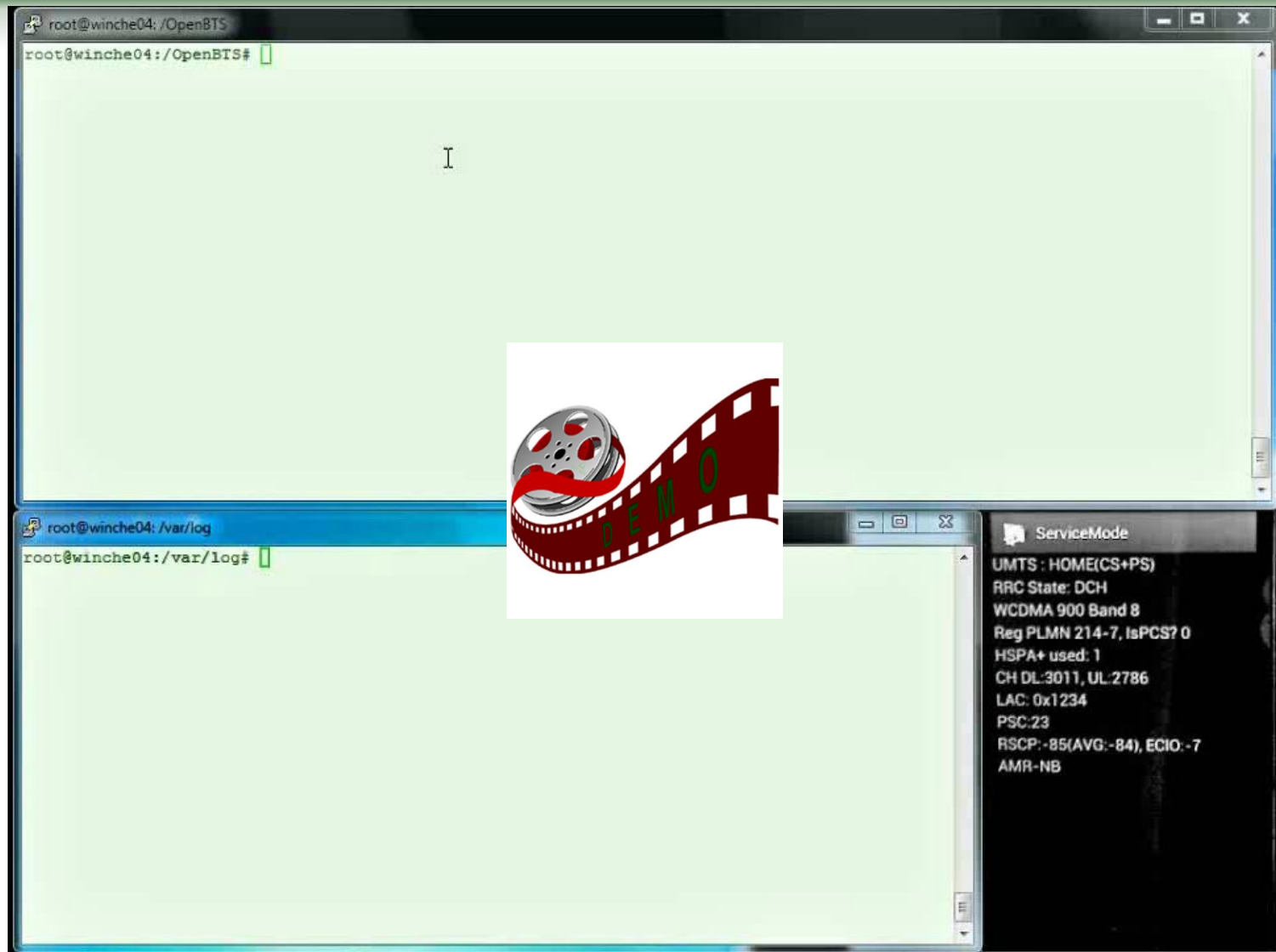
- ▶ Determina la presencia de un usuario en la zona

¿Qué se necesita?

- ▶ Una infraestructura de estación base falsa como la descrita anteriormente, sin necesidad de modificaciones *software*.



IMSI Catching




















Denegación de servicio persistente y selectiva

La técnica de LURCC aplicada a 3G
(RAURCC)



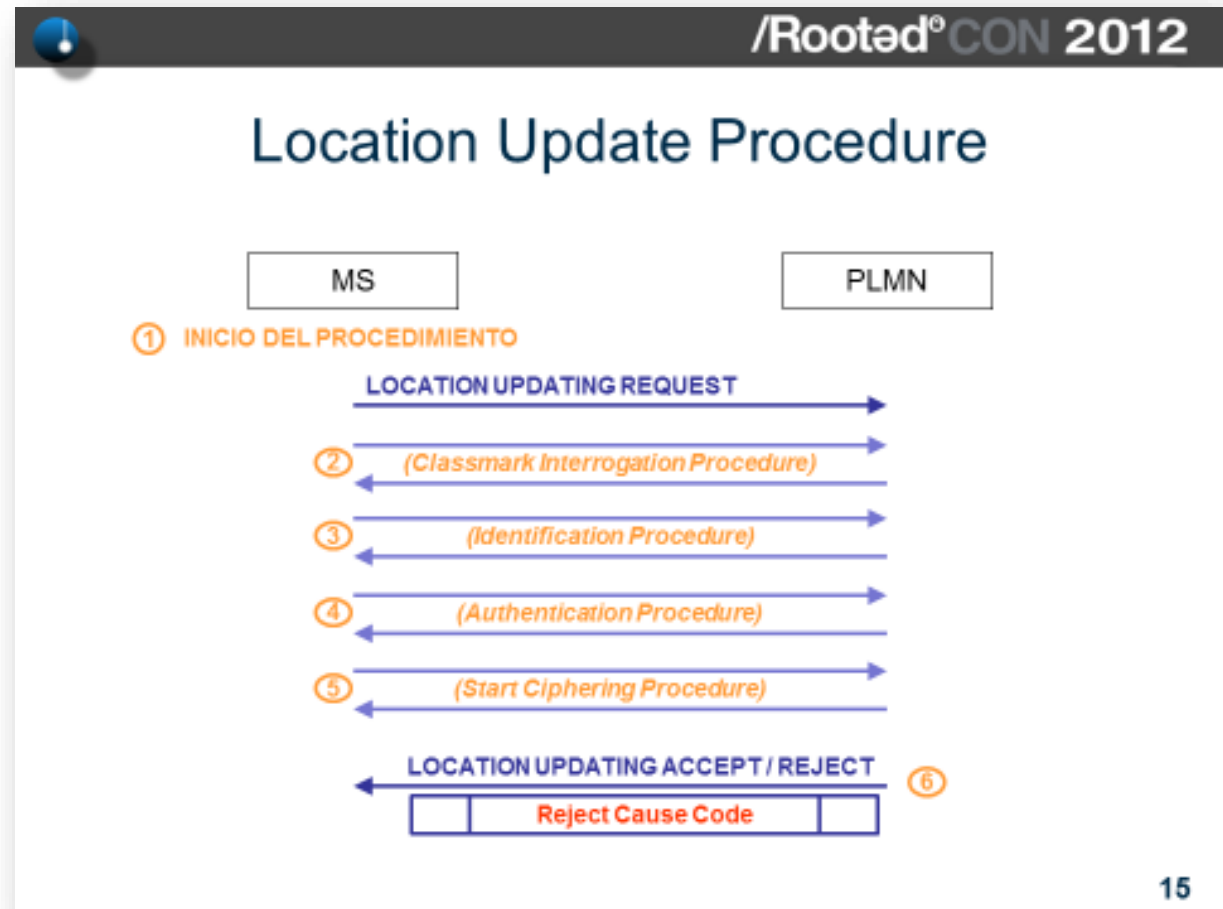
Denegación de servicio de telefonía móvil

Diferentes técnicas

	Ataque Masivo	Ataque Selectivo	Ataque Persistente	Transparente al usuario
Inhibidor de frecuencia				
Agotamiento de canales de radio en la BTS				
Redirección mediante estación base falsa				
Técnica LUPRCC				 

Técnica LURCC (RAURCC)

Fundamentos teóricos





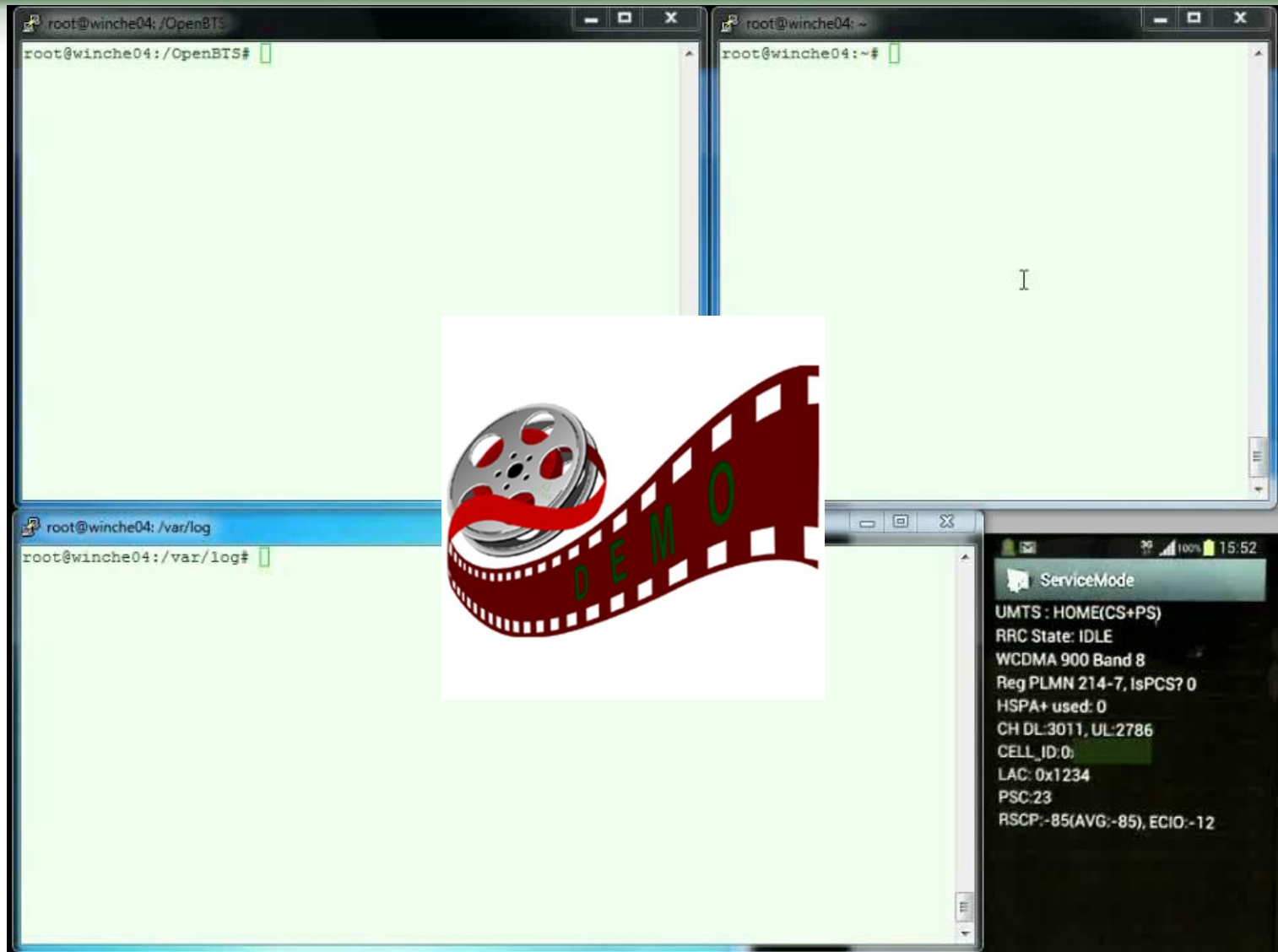
Técnica LURCC (RAURCC)

¿Qué se necesita?

- ▶ Una infraestructura de estación base falsa UMTS como la descrita anteriormente
- ▶ Una modificación del software de la estación base falsa para que pueda implementar el ataque de forma selectiva y configurable



RAURCC: “Illegal MS”





Escenario de aplicación





Escenario de aplicación



Trabajos en curso y a futuro

Qué es lo que estamos haciendo ahora y
qué queríamos hacer en el futuro...



Geolocalización

Objetivo del Sistema



LACON¹²

4



Geolocalización

Trabajo en curso

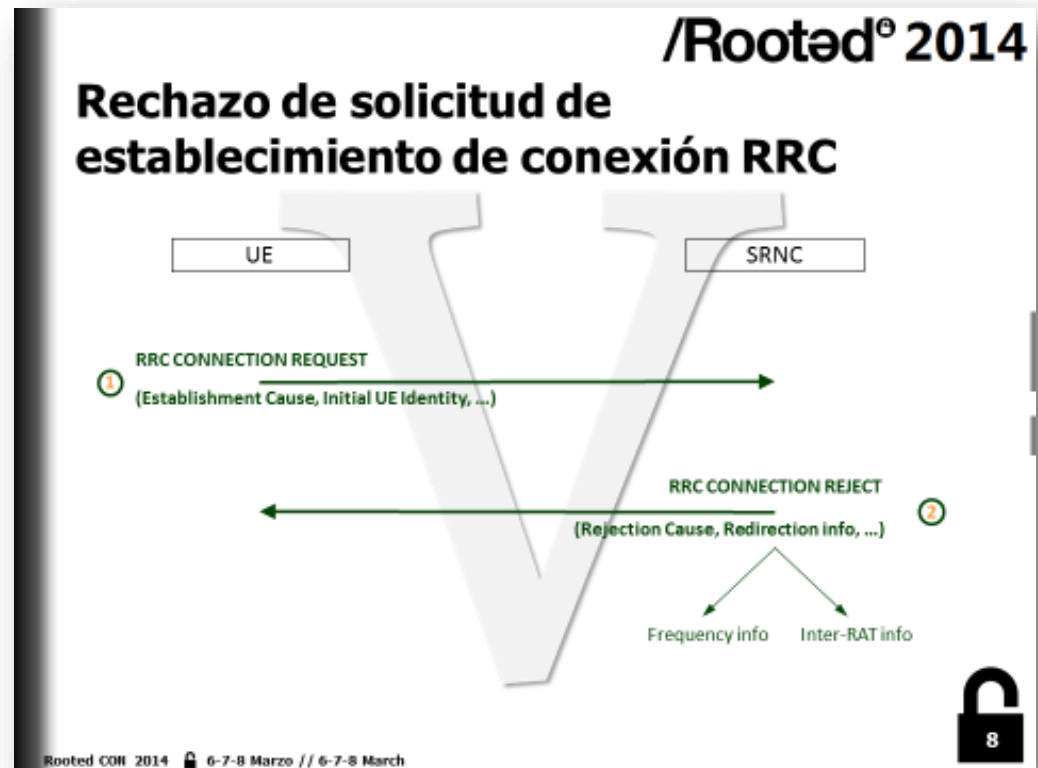
- ▶ Portar el sistema ya realizado a 3G
 - ▶ modificar la estación base para que mantenga los canales de radio abiertos el mayor tiempo posible
 - ▶ obtener datos para triangular similares a los usados en 2G
- ▶ ¿Otros caminos?



Downgrade selectivo a 2G

Trabajo en curso

- Desarrollo de la funcionalidad necesaria dentro de OpenBTS-UMTS para probar las técnicas descritas en RootedCON2014





Trabajo futuro

- ▶ Continuar el trabajo del sniffer 3G
- ▶ Probar estas técnicas en tecnología 4G
- ▶ Estudiar las implicaciones del cambio de SIM a eSIM

CONCLUSIONES



Conclusiones

- ▶ Ataques demostrados ya en la práctica:
 - ▶ IMSI Catching 3G
 - ▶ Denegación de servicio persistente y selectiva 3G
- ▶ Ataques por demostrar en la práctica (en breve):
 - ▶ geolocalización
 - ▶ *downgrade* selectivo 3G → 2G

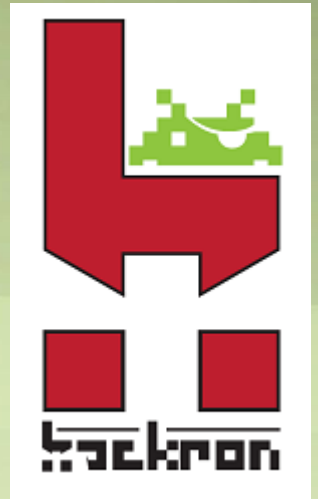
¡ Muchas gracias !





www.layakk.com

@layakk



3G Attacks

José Picó García
(David Pérez Conde)