/Rootəd 2012

Nuevos escenarios de ataque con estación base falsa GSM/GPRS

#rootedgsm

Taddong

www.taddong.com
@taddong

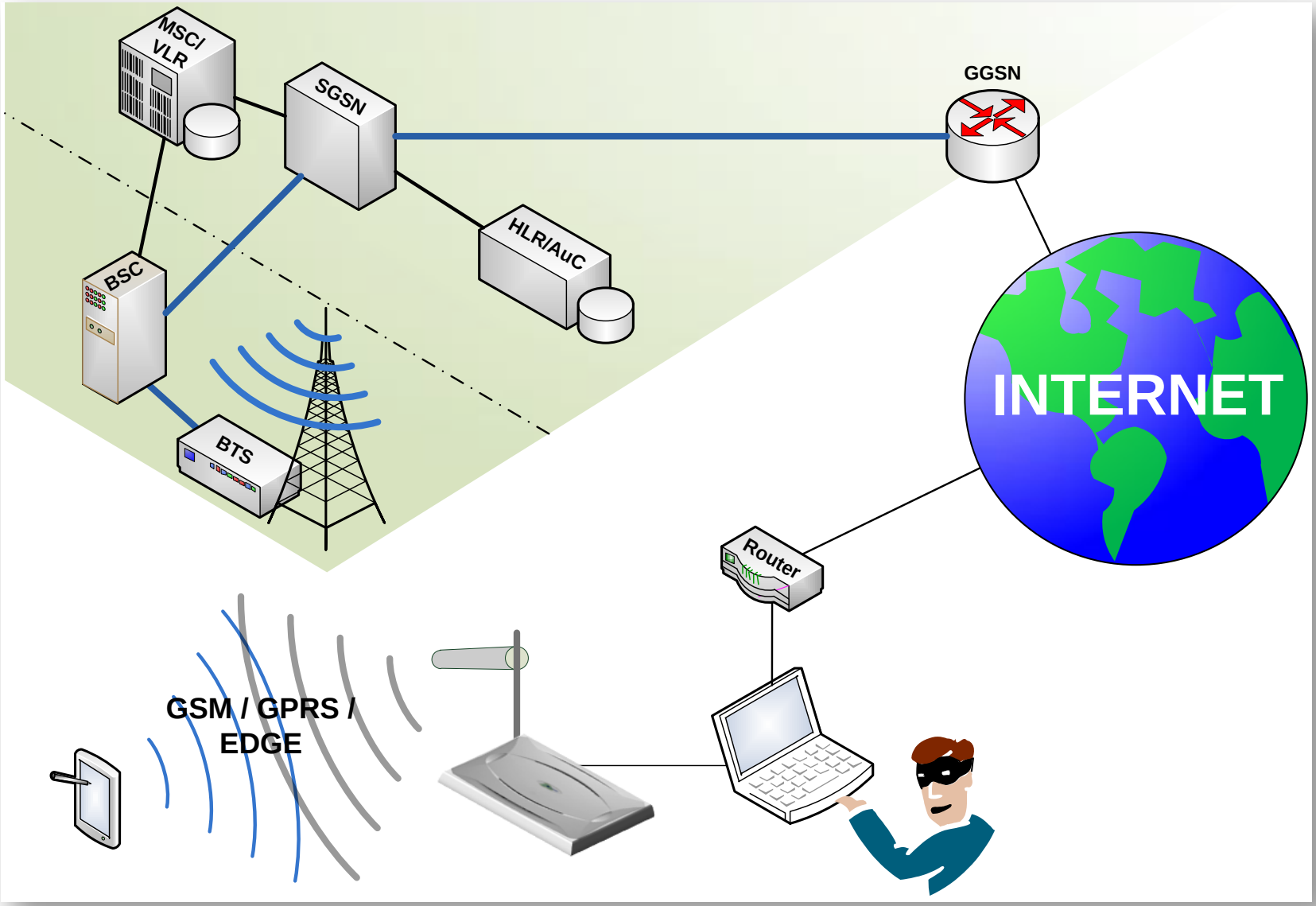
José Picó - jose@taddong.com
David Pérez - david@taddong.com

Introducción

Terminología

- **BTS** – *Base Station Transceiver*:
  - Estación base; estación de radio que constituye el acceso del móvil a la red
- **PLMN** – *Public Land Mobile Network*:
  - El operador de telefonía
- **HPLMN** – *Home PLMN*:
  - Es el operador que emite una tarjeta SIM y el único que conoce su clave precompartida Ki
- **IMSI** – *International Mobile Subscriber Identifier*:
  - Identificar único de la tarjeta SIM (y del usuario)
- **TMSI** – *Temporary Mobile Subscriber Identifier*:
  - Identificador temporal asignado por la red para que el móvil no tenga que revelar su IMSI constantemente

Ataque con estación base falsa



Ataque con estación base falsa

Voz

- Grabación de llamadas y SMS
- Suplantación número llamante
- Suplantación destino (redirección)
- Impersonación del usuario

Datos

- Interceptación de tráfico
- Redirección de tráfico
- Posición privilegiada para realizar todo tipo de ataques IP

Escenario objeto de esta charla

Escenario objeto de esta charla

Denegación de servicio de telefonía móvil

Denegación de Servicio GSM

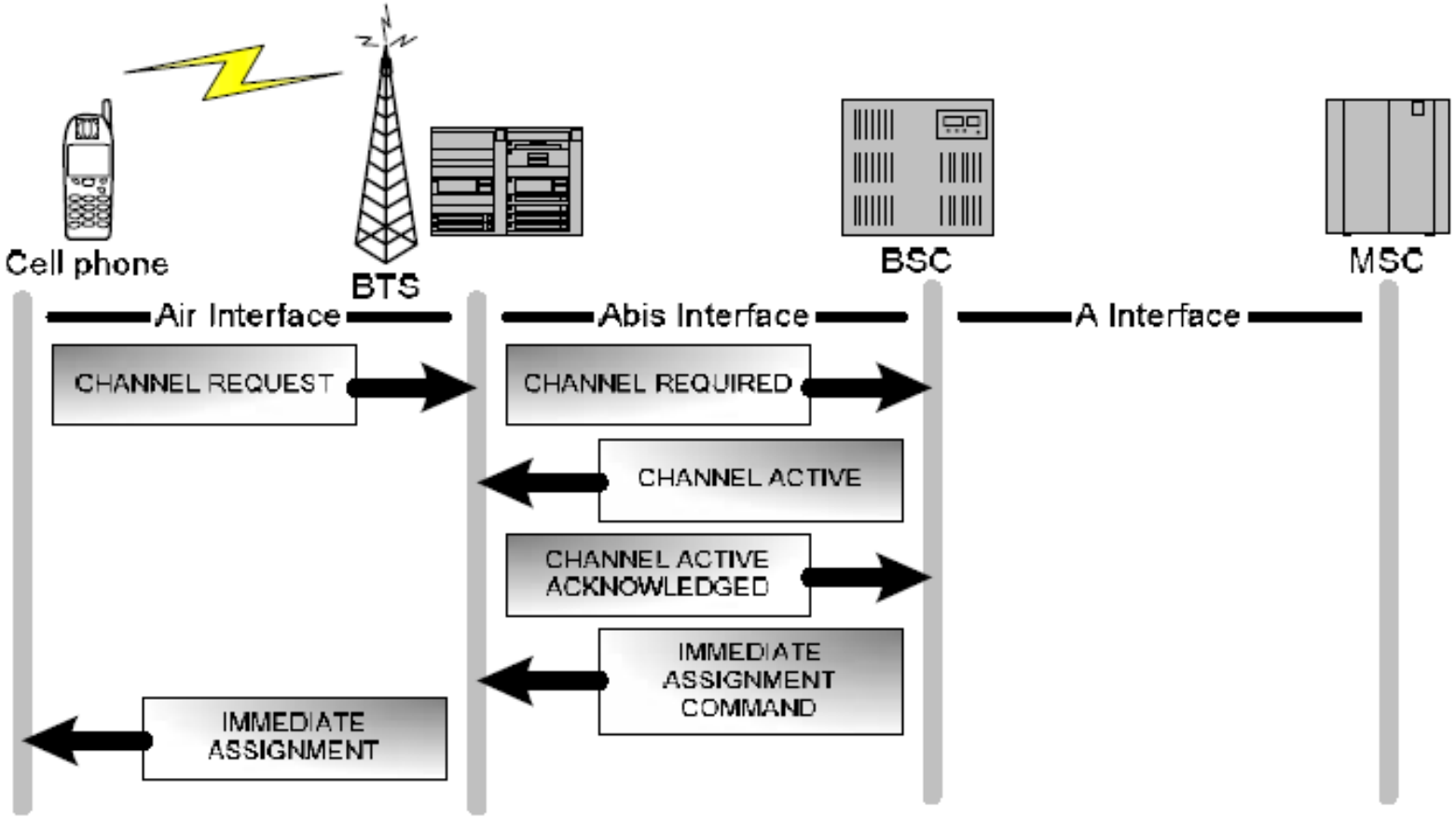
Características de los ataques de denegación de servicio de telefonía móvil

Ataque 'Masivo'	El ataque es capaz de causar una denegación de servicio de forma masiva e indiscriminada en el alcance del sistema.
Ataque 'Selectivo'	El ataque es capaz de causar una denegación de servicio selectivamente sólo a algunos terminales móviles que pueden ser discriminados por el atacante.
Ataque 'Persistente'	El ataque persiste en el tiempo (hasta una determinada condición) después de que el atacante deja de actuar y sale del lugar.
Ataque 'Transparente'	El usuario no percibe ninguna señal de que ha perdido el servicio

Comparativa de técnicas para llevar a cabo una denegación de servicio GSM

	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	✓	✓	✓	✗

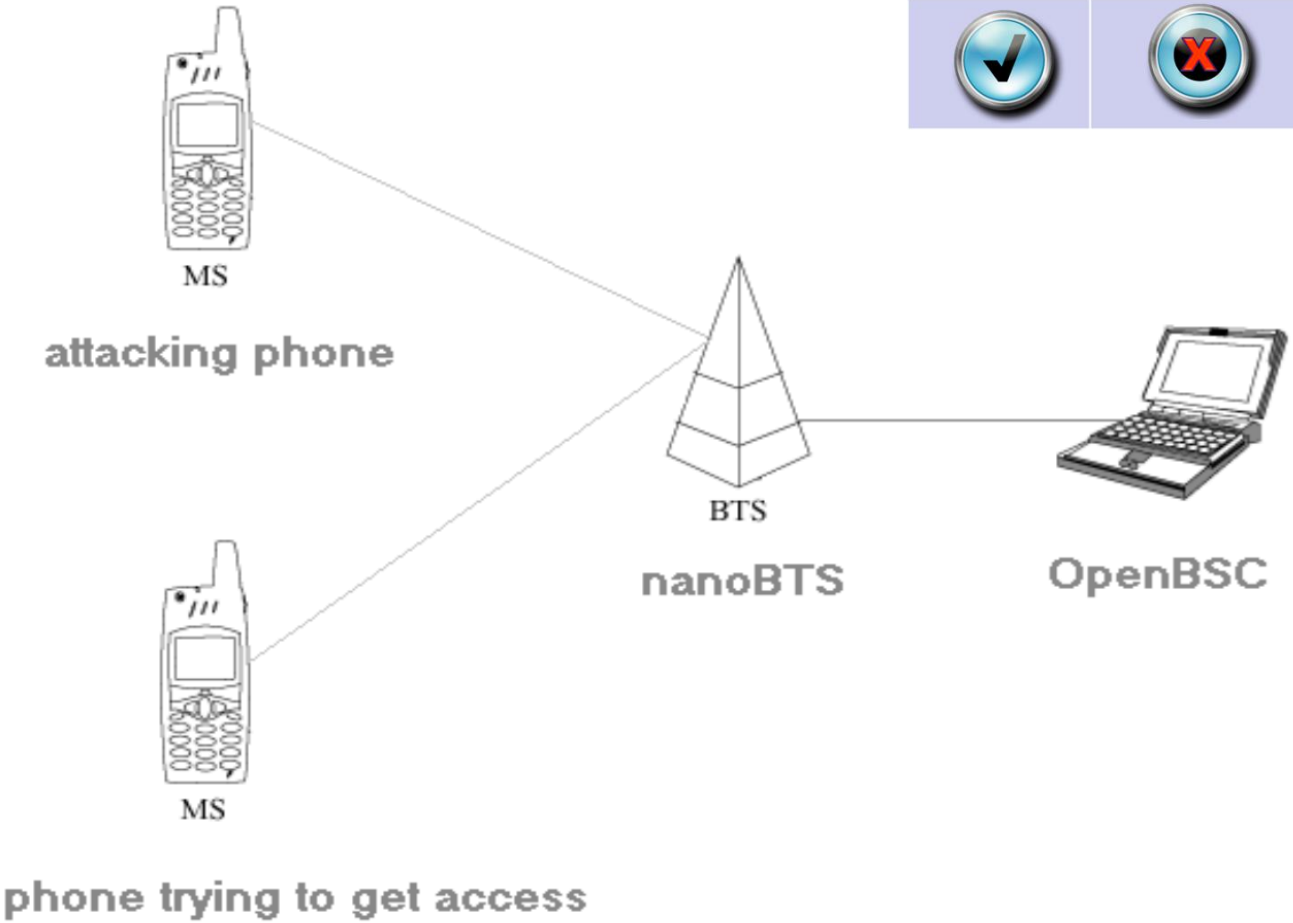
Agotamiento de canales de radio en la BTS (I)



Ref.: “Threats and countermeasures in GSM networks”. Valer Bocan, Bocan Cretu
http://ojs.academypublisher.com/index.php/jnw/article/view/010618/655

Agotamiento de canales de radio en la BTS (II)

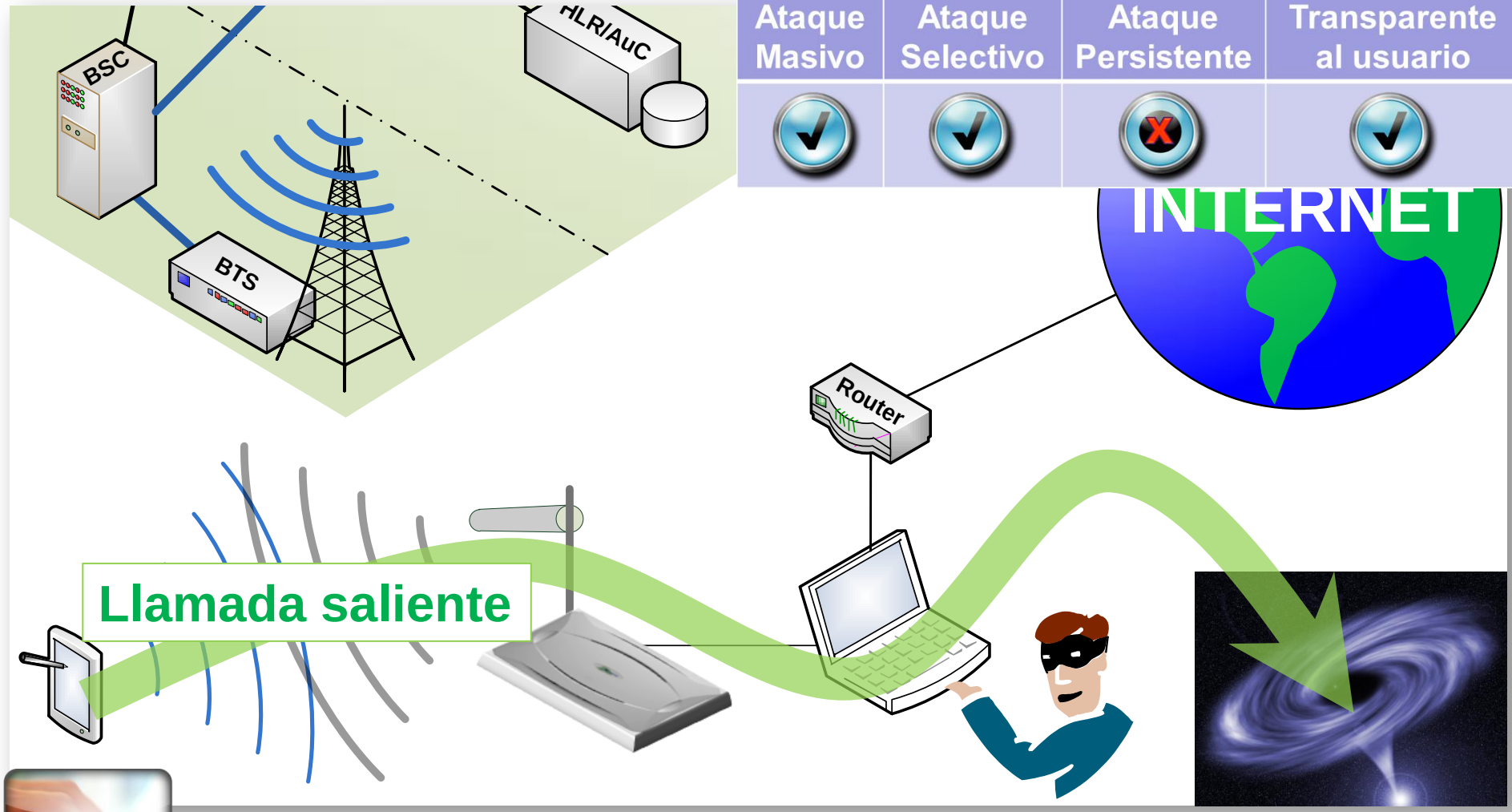
Ataque Masivo	Ataque Selectivo	Ataque Persistente	Transparente al usuario
✓	✗	✗	✗



Ref.: “A practical DoS attack to the GSM Network”. Dieter Spaar.
http://www.mirider.com/GSM-DoS-Attack_Dieter_Spaar.pdf

Redireccion mediante estación base falsa

Ataque Masivo	Ataque Selectivo	Ataque Persistente	Transparente al usuario
✓	✓	✗	✓



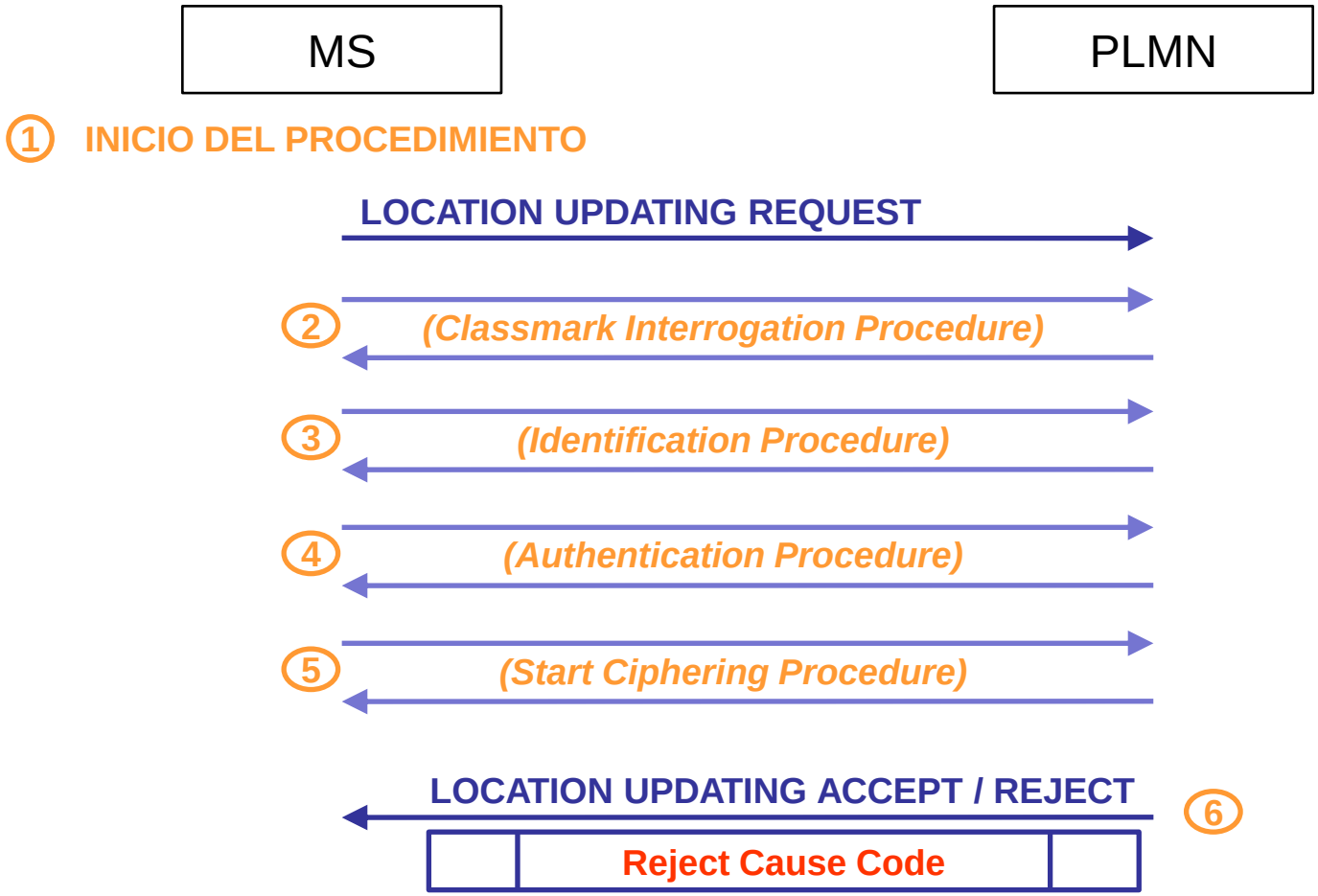
Demo

Denegación de Servicio GSM

Técnica LUPRCC

(Location Update Procedure Reject Cause Codes)

Location Update Procedure



Location Update Procedure Reject Cause Codes

Dec	Hex	Descripción
02	0x02	IMSI unknown in HLR
03	0x03	Illegal MS
06	0x06	Illegal ME
11	0x0B	PLMN not allowed
12	0x0C	Location Area not allowed
13	0x0D	Roaming not allowed in this location area
15	0x0F	No Suitable Cells In Location Area
OTHER	OTHER	OTHER

Location Update Procedure Reject Cause Codes

Dec	Hex	Descripción
02	**0x02**	**IMSI unknown in HLR**
03	**0x03**	**Illegal MS**
06	**0x06**	**Illegal ME**
11	**0x0B**	**PLMN not allowed**
12	0x0C	Location Area not allowed
13	0x0D	Roaming not allowed in this location area
15	0x0F	No Suitable Cells In Location Area
OTHER	**OTHER**	**OTHER**

Comportamiento descrito por la norma ante LU Reject

Cause Code: OTHER (sólo por curiosidad)

3GPP TS 24.008 - 4.4.4.7

"The MS waits for release of the RR connection as specified in sub-clause 4.4.4.8, and then proceeds as follows. TimerT3210 is stopped if still running. The RR Connection is aborted in case of timer T3210 timeout. The attempt counter isincremented. The next actions depend on the Location Area Identities (stored and received from the BCCH of thecurrent serving cell) and the value of the attempt counter."

"– the update status is UPDATED, and the stored LAI is equal to the one received on the BCCH from the currentserving cell and the attempt counter is smaller than 4:The mobile station shall keep the update status to UPDATED, the MM IDLE sub-state after the RR connection release is NORMAL SERVICE. The mobile station shall memorize the location updating type used in the location updating procedure. It shall start timer T3211 when the RR connection is released. When timer T3211 expires the location updating procedure is triggered again with the memorized location updating type;"

"– either the update status is different from UPDATED, or the stored LAI is different from the one received on theBCCH from the current serving cell, or the attempt counter is greater or equal to 4:The mobile station shall delete any LAI, TMSI, ciphering key sequence number stored in the SIM, set the updatestatus to NOT UPDATED and enter the MM IDLE sub-state ATTEMPTING TO UPDATE when the RRconnection is released (See sub-clause 4.2.2.2 for the subsequent actions). If the attempt counter is smaller than4, the mobile station shall memorize that timer T3211 is to be started when the RR connection is released,otherwise it shall memorize that timer T3212 is to be started when the RR connection is released."

Comportamiento descrito por la norma ante LU Reject

Cause Code: 0x0B (PLMN not allowed)

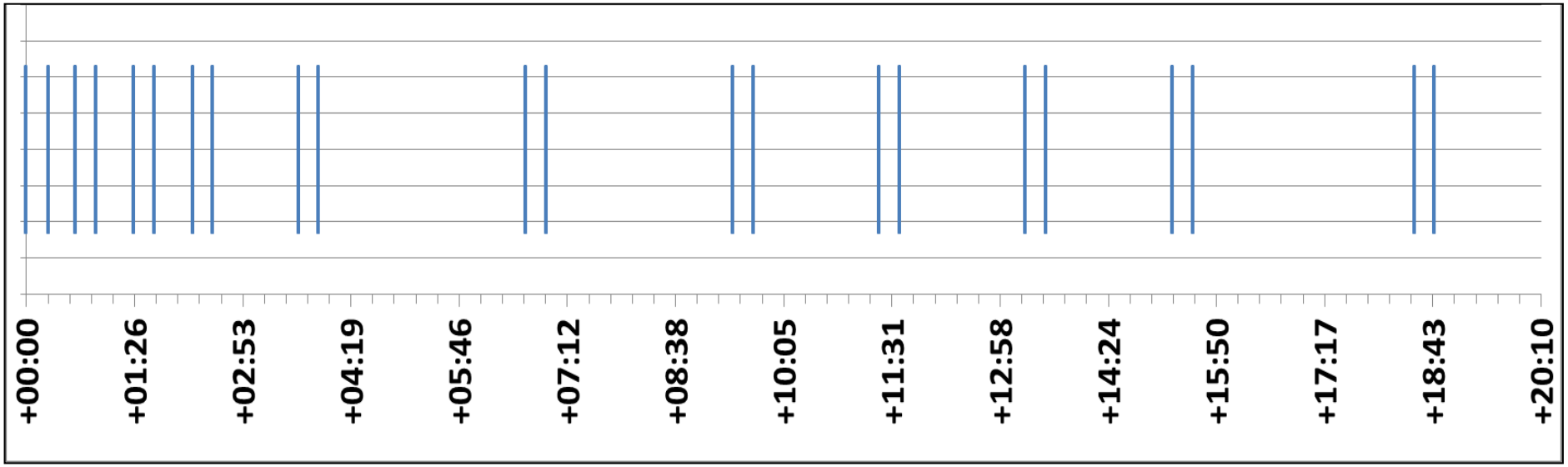
3GPP TS 24.008 - 4.4.4.7

"The mobile station shall delete any LAI, TMSI and ciphering key sequence number stored in the SIM/USIM, reset the attempt counter, and set the update status to ROAMING NOT ALLOWED (and store it in the SIM/USIM according to subclause 4.1.2.2). The mobile station shall store the PLMN identity in the 'forbidden PLMN list'.The MS shall perform a PLMN selection when back to the MM IDLE state according to 3GPP TS 23.122. An MS in GAN mode shall request a PLMN list in GAN (see 3GPP TS 44.318) prior to performing a PLMN selection from this list according to 3GPP TS 23.122."

Pruebas de comportamiento ante LU Reject

Cause Code: 0x0B (PLMN not allowed)

Intentos de conexión del móvil en el tiempo desde el primer rechazo



Comportamiento descrito por la norma ante LU Reject

Cause Code: 0x02 (IMSI unknown in HLR)

Cause Code: 0x03 (Illegal MS)

Cause Code: 0x05 (Illegal ME)

3GPP TS 24.008 - 4.4.4.7

"The mobile station shall set the update status to ROAMING NOT ALLOWED (and store it in the SIM/USIM according to subclause 4.1.2.2), and delete any TMSI, stored LAI and ciphering key sequence number and shall consider the SIM/USIM as invalid for non-GPRS services until switch-off or the SIM/USIM is removed."

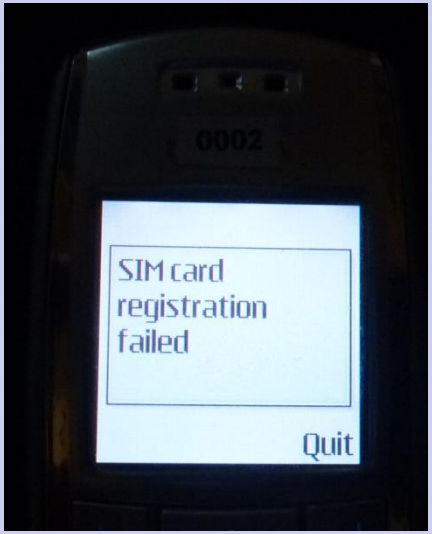
Pruebas de comportamiento ante LUReject

Terminales probados en el laboratorio

	0x02 IMSI unknown in HLR	0x03 Illegal MS	0x06 Illegal ME
Nokia 6210 (Simyo)			

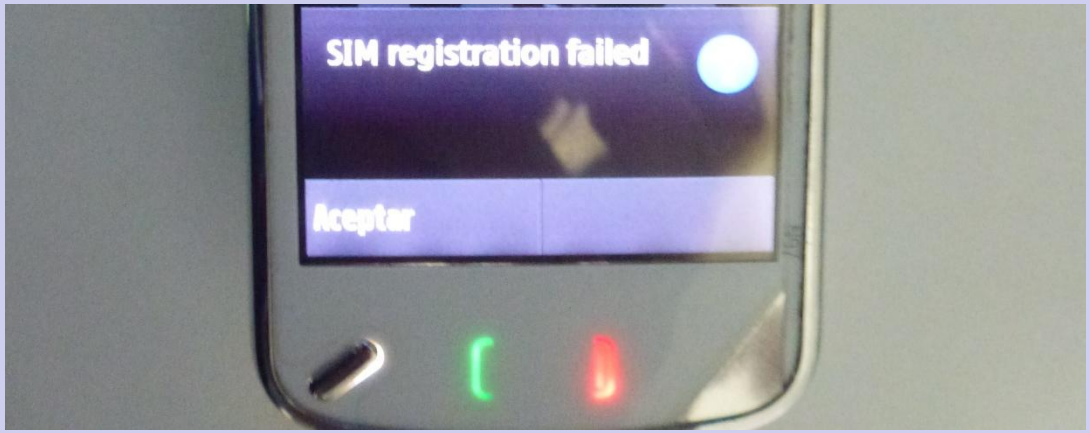
Pruebas de comportamiento ante LUReject

Terminales probados en el laboratorio

	0x02 IMSI unknown in HLR	0x03 Illegal MS	0x06 Illegal ME
Nokia 3210 (Simyo)			

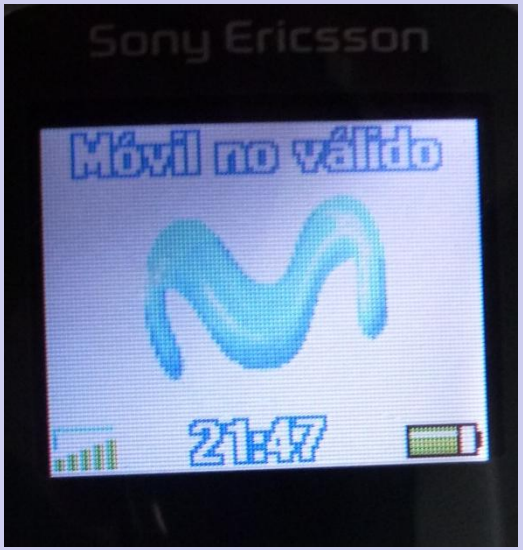
Pruebas de comportamiento ante LUReject

Terminales probados en el laboratorio

	0x02 IMSI unknown in HLR	0x03 Illegal MS	0x06 Illegal ME
Nokia N97(Movistar)			

Pruebas de comportamiento ante LUReject

Terminales probados en el laboratorio

	0x02 IMSI unknown in HLR	0x03 Illegal MS	0x06 Illegal ME
Sony-Ericsson T290i (Movistar)			

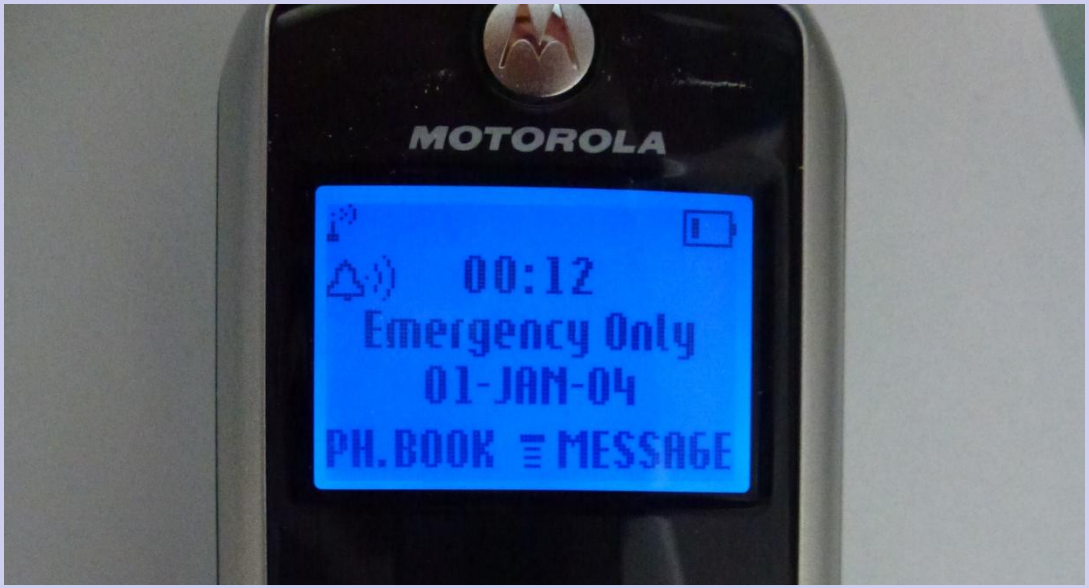
Pruebas de comportamiento ante LUReject

Terminales probados en el laboratorio

	0x02 IMSI unknown in HLR	0x03 Illegal MS	0x06 Illegal ME
Siemens A55 (Simyo)			

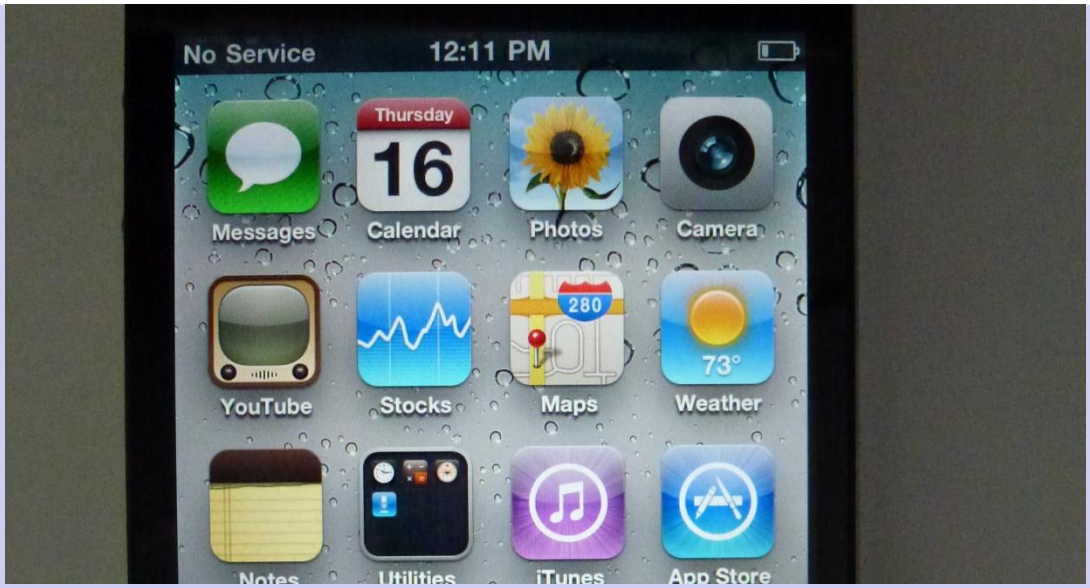
Pruebas de comportamiento ante LUReject

Terminales probados en el laboratorio

	0x02 IMSI unknown in HLR	0x03 Illegal MS	0x06 Illegal ME
Motorola C123 (Simyo)			

Pruebas de comportamiento ante LUReject

Terminales probados en el laboratorio

	0x02 IMSI unknown in HLR	0x03 Illegal MS	0x06 Illegal ME
iPhone (Movistar)			

Pruebas de comportamiento ante LU Reject

- Cause Code: 0x02 (IMSI unknown in HLR)
- Cause Code: 0x03 (Illegal MS)
- Cause Code: 0x05 (Illegal ME)

Demo

Vídeo

Escenario de aplicación

El ataque puede ser un ataque masivo

- El atacante puede rechazar indiscriminadamente los intentos de conexión, sea cual sea el identificador de las víctimas
- La capacidad de proceso no es determinante (el atacante sólo debe rechazar un registro de cada víctima)
- Se puede realizar consecutivamente a varios operadores (o simultáneamente con varios equipos iguales)

El ataque puede ser un ataque selectivo

Sólo es necesario poder identificar a la SIM (IMSI o TMSI) de la víctima

- Existen varias técnicas para identificar a la víctima, por ejemplo:
  - Técnicas de “monitorización” para obtener el IMSI: http://blog.taddong.com/2011/05/selective-attack-with-rogue-gsmgprs.html
  - Descubrir el TMSI y utilizarlo: http://events.ccc.de/congress/2011/Fahrplan/attachments/1994_111217.SRLabs-28C3-Defending_mobile_phones.pdf
  - Interrogar al HLR a través de la red global SS7: http://events.ccc.de/congress/2010/Fahrplan/attachments/1783_101228.27C3.GSM-Sniffing.Nohl_Munaut.pdf

La denegación es persistente

- El terminal no recupera el servicio hasta que el usuario lo apaga y lo enciende de nuevo

La denegación NO es transparente

- El mensaje al usuario depende del terminal: algunos terminales muestran en pantalla un mensaje para informar al usuario y otros simplemente que no hay cobertura

Contramedidas

Protección de los mensajes de nivel 3 en UMTS

- En todas las conexiones de control N3 establecidas es obligatorio iniciar el procedimiento de protección de integridad de los mensajes de señalización. Existen 5 excepciones a esta norma (*3GPP 33.102*), que no aplican al Location Registration Reject procedure; explícitamente se describe "*(…)it shall be mandatory for the VLR/SGSN to start integrity protection before sending a reject signalling message that causes the CSG list on the UE to be modified (…)*".
- El procedimiento de protección de integridad se establece mediante el *security mode command*

Contramedidas

USUARIOS

Prohibir en nuestros terminales el uso de 2G

OPERADORES

Desplegar completamente 3G/4G y eliminar la cobertura 2G

Conclusión

/Rootəd 2012

Nuevos escenarios de ataque con estación base falsa GSM/GPRS

#rootedgsm

Taddong

www.taddong.com
@taddong

José Picó - jose@taddong.com
David Pérez - david@taddong.com