

/Rootəd[🔒] 2016

Atacando 3G vol. III



www.layakk.com
@layakk

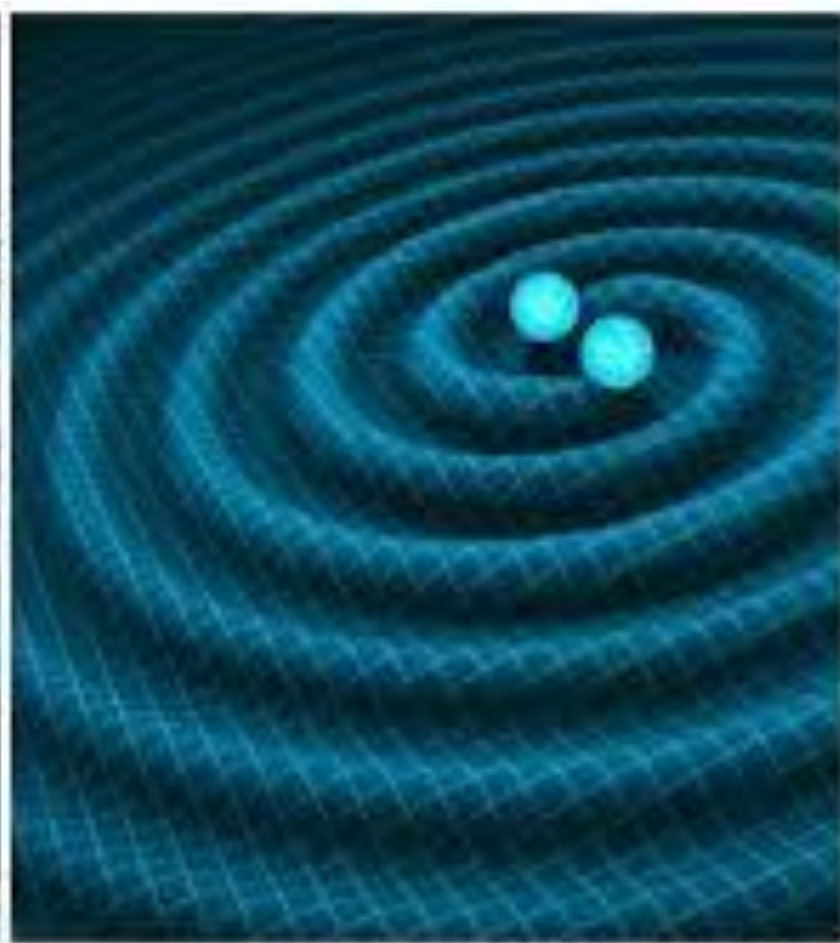
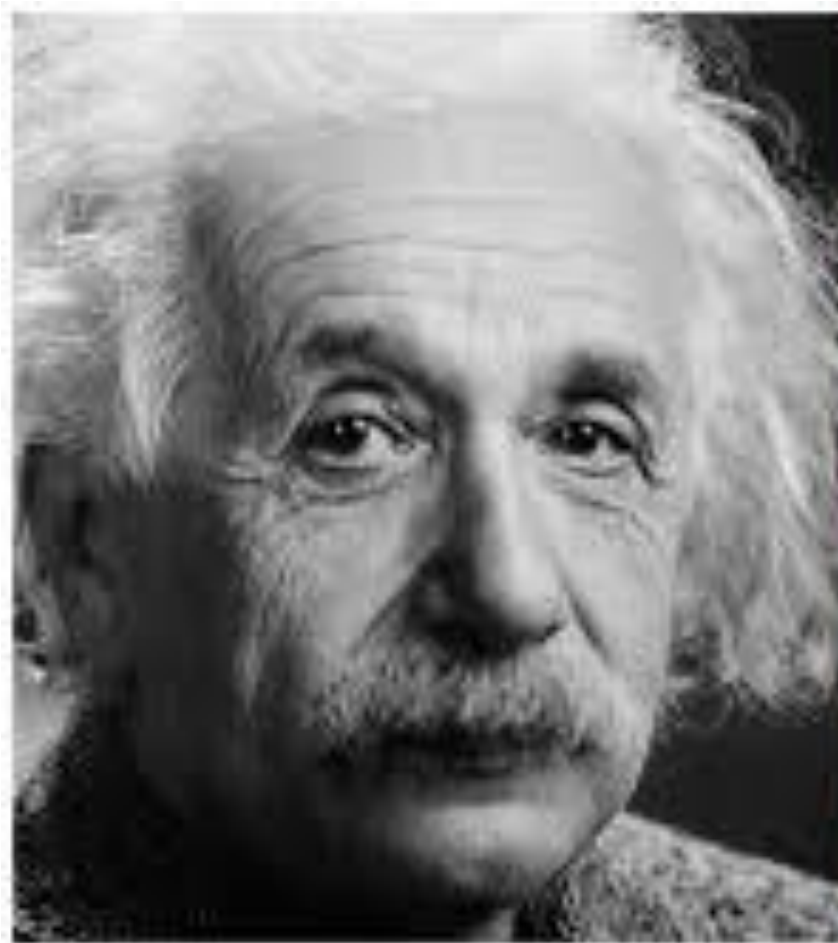
José Picó
David Pérez

jose.pico@layakk.com
david.perez@layakk.com



Objetivo

Es el año de saldar cuentas pendientes...



Objetivo

Es el año de saldar cuentas pendientes...



Objetivo

Es el año de saldar cuentas pendientes...

/Rooted[®] 2014

Conclusiones

- 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.

Ataques 3G (estación base falsa)

- IMSI Catching *creemos que* es posible
- Geolocalización de dispositivos *creemos que* es posible
- Denegación de servicio *creemos que* es posible
- Downgrade selectivo a 2G *creemos que* es posible

El ataque en la práctica

IMSI CATCHING 3G

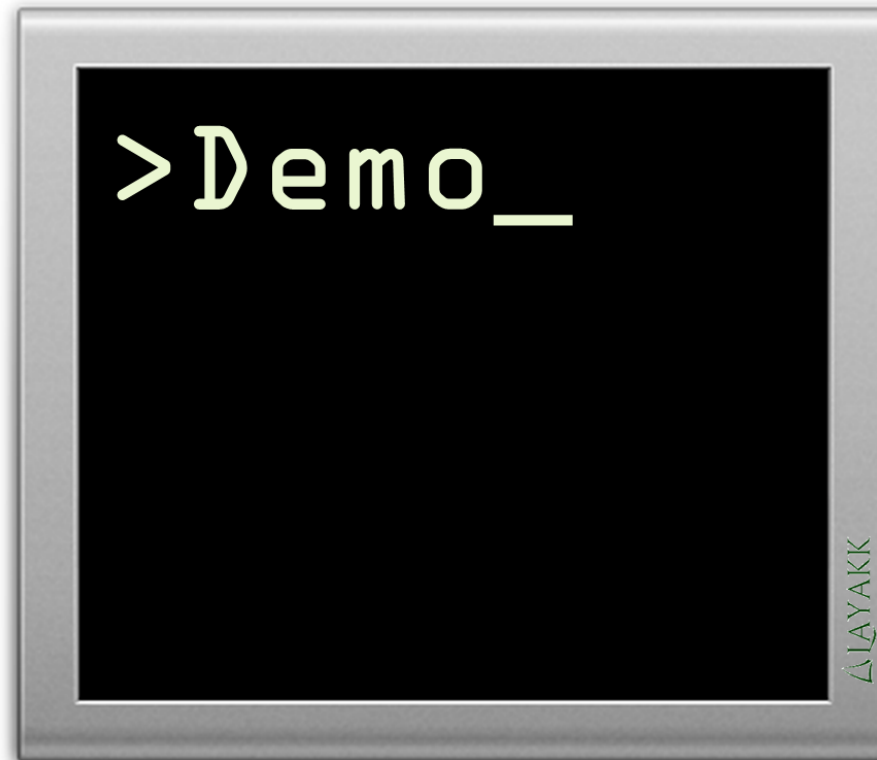
UMTS IMSI Catching

- Captura no autorizada de IMSIs
- Determina la presencia de un usuario en la zona
- Se necesita:
 - Una infraestructura de estación base falsa
 - Software de monitorización para la configuración adecuada de la celda falsa, basado en *xgoldmon*

Ref.: <http://openbts.org/w/index.php?title=OpenBTS-UMTS>

Ref.: <https://github.com/2b-as/xgoldmon>

Caracterización UMTS



UMTS IMSI Catching

/Rooted° 2014

Mensajes de señalización RRC no protegidos en integridad

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

• RRC CONNECTION REQUEST

• RRC CONNECTION SETUP

• IDENTITY REQUEST



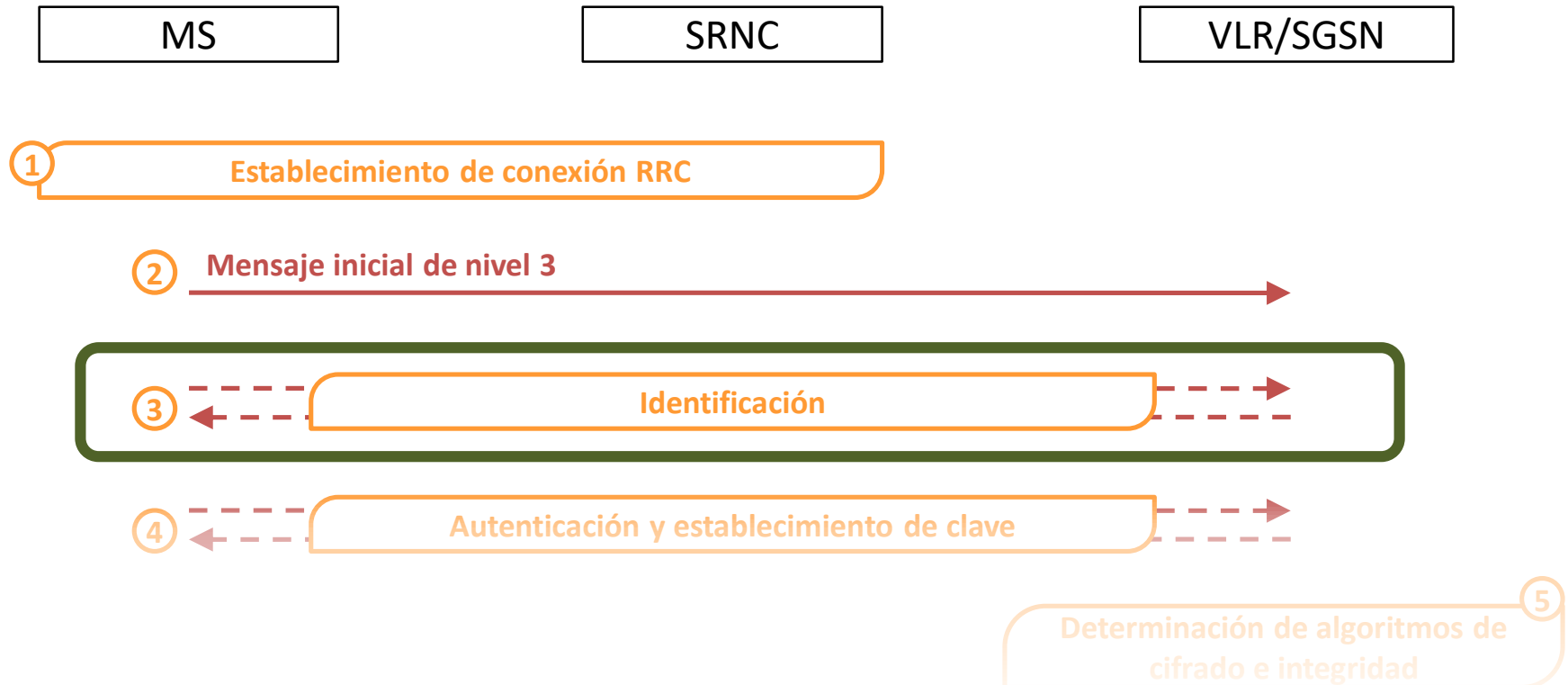
/Rooted° 2014

Mensajes MM (DL) permitidos antes del security mode command

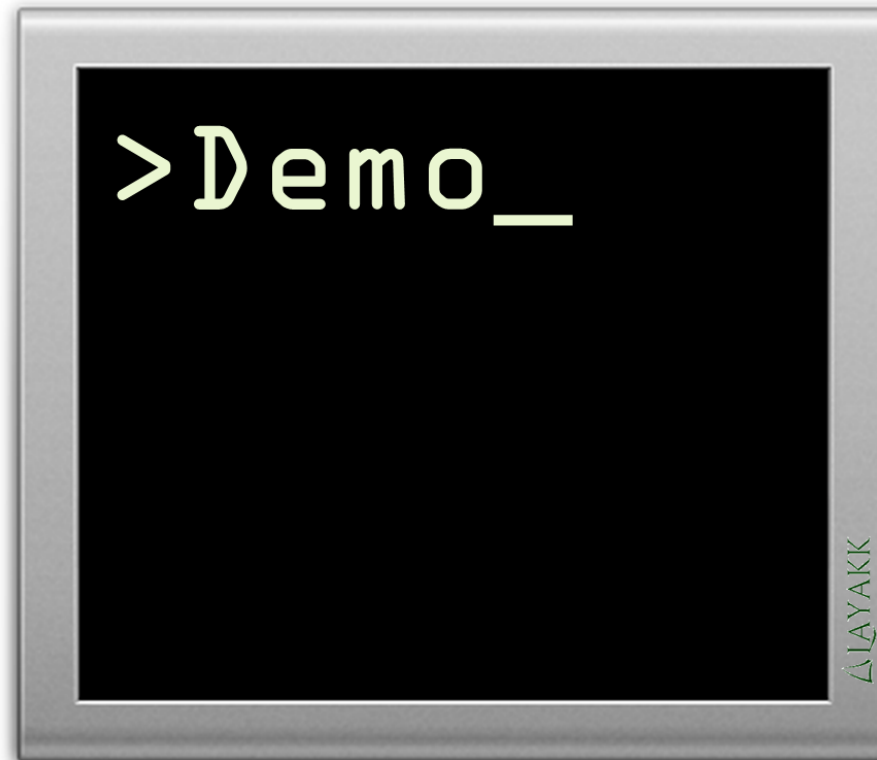
- AUTHENTICATION REQUEST
- AUTHENTICATION REJECT
- IDENTITY REQUEST
- LOCATION UPDATING REJECT
- LOCATION UPDATING ACCEPT (at periodic location update with change of location area or temporary identity)
- CM SERVICE ACCEPT, if the following two conditions apply:
 - no other MM connection is established; 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



UMTS IMSI Catching



UMTS IMSI Catching



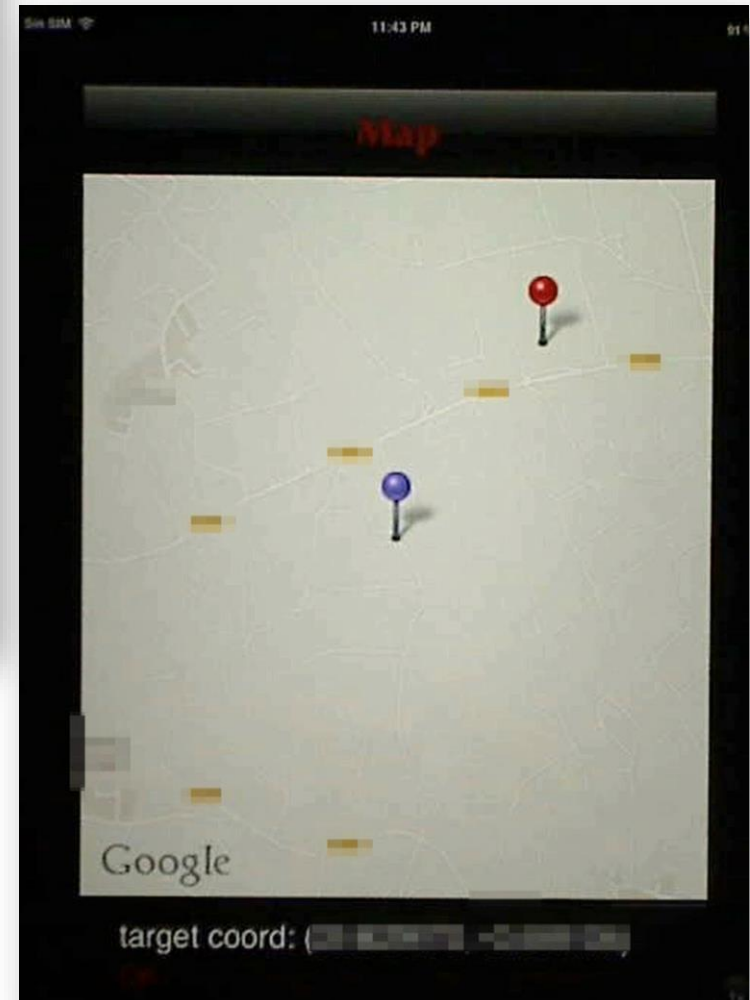
Ataques 3G (estación base falsa)

- IMSI Catching creemos que es posible
- Geolocalización de dispositivos creemos que es posible
- Denegación de servicio persistente creemos que es posible
- Downgrade selectivo a 2G creemos que es posible

Técnicas de obtención de datos de señalización en el *uplink*

GEOLOCALIZACIÓN DE DISPOSITIVOS

Geolocalización de terminales móviles

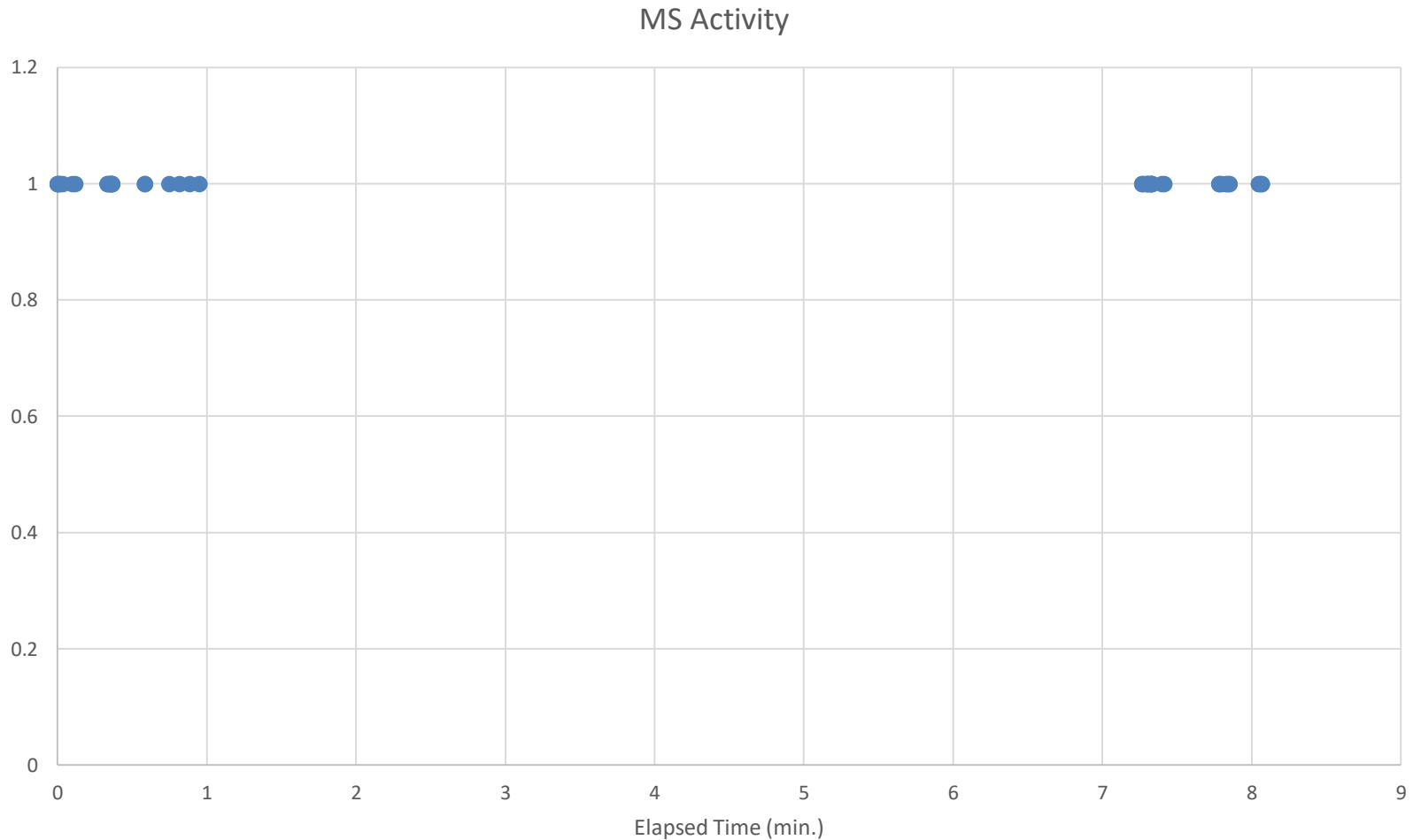


Obtención de datos para el cálculo

- En la versión 2G lo hacíamos con un canal de radio dedicado y permanente:
 - ✓ Llegan medidas continuamente
 - ✗ Es difícil mantener el canal abierto debido a la distancia, zonas de sombra, etc.
- En 3G no podemos establecer un canal de radio permanente

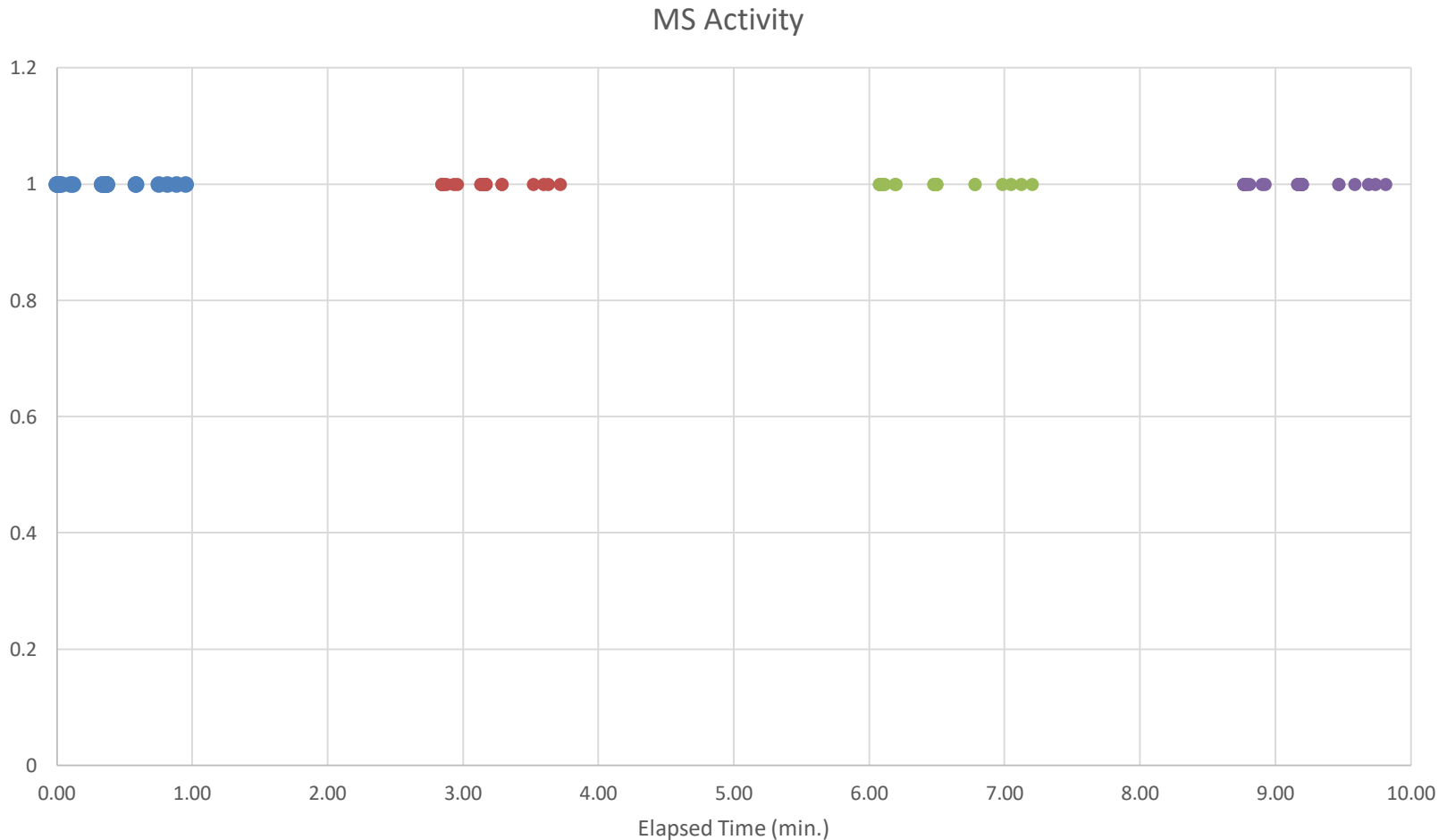
Obtención de datos para el cálculo

Actividad en el *uplink* de una MS






Mejora en la recepción de datos

Actividad en el *uplink* de una MS



Geolocalización: conclusión

- El número de muestras útiles para calcular la posición es menor y más espaciado en el tiempo (como se esperaba):
 -  El proceso se ralentiza
 -  El grado de precisión se reduce ligeramente
- No obstante:
 -  La geolocalización mediante esta técnica es totalmente viable

Ataques 3G (estación base falsa)


















- IMSI Catching es posible
- Geolocalización de dispositivos es posible *) creemos que*
- Denegación de servicio persistente es posible *) creemos que*
- Downgrade selectivo a 2G es posible *) creemos que*

El ataque RAUPRCC en la práctica

DENEGACIÓN DE SERVICIO

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				 

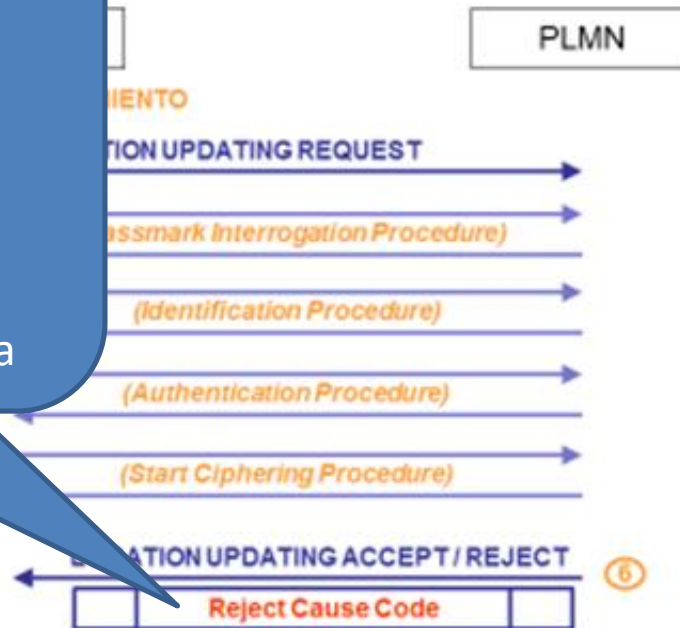
Denegación de servicio de telefonía móvil

Location Update Procedure Reject Cause Code

/Rooted[®]CON 2012

Location Update Procedure

IMSI unknown in HLR
Illegal MS
Illegal ME
PLMN not allowed
Location Area not allowed
Roaming not allowed in this
location area
No Suitable Cells In Location Area



UMTS Denial of Service

Routing Area Update Procedure Reject Cause Code:
“Illegal MS”



Escenario de aplicación



Escenario de aplicación



Ataques 3G (estación base falsa)

- IMSI Catching es posible
- Geolocalización de dispositivos es posible
- Denegación de servicio persistente es posible *) creemos que*
- Downgrade selectivo a 2G es posible *) creemos que*

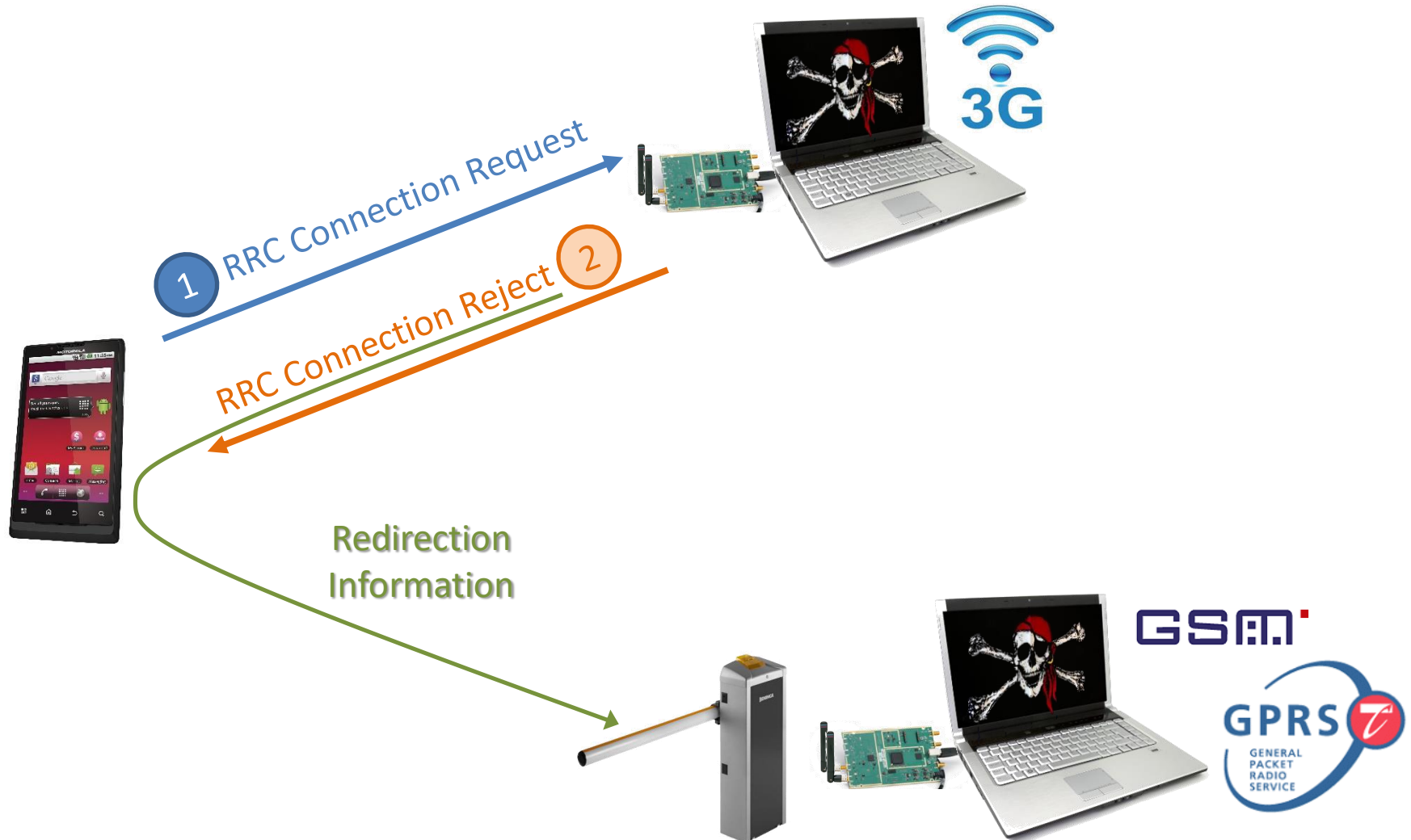
El ataque en la práctica

***DOWNGRADE* SELECTIVO A 2G**

Downgrade selectivo a 2G

- En 3G el ataque completo con estación base falsa no es posible
- Para hacer *downgrade* a 2G, es posible utilizar un inhibidor. Problemas:
 - Alcance
 - Filtrado adecuado de las bandas
 - Consumo / disipación de calor
 - Interferencia con dispositivos propios (del atacante)
 - Detectable más fácilmente
 - No puede hacerse de forma selectiva

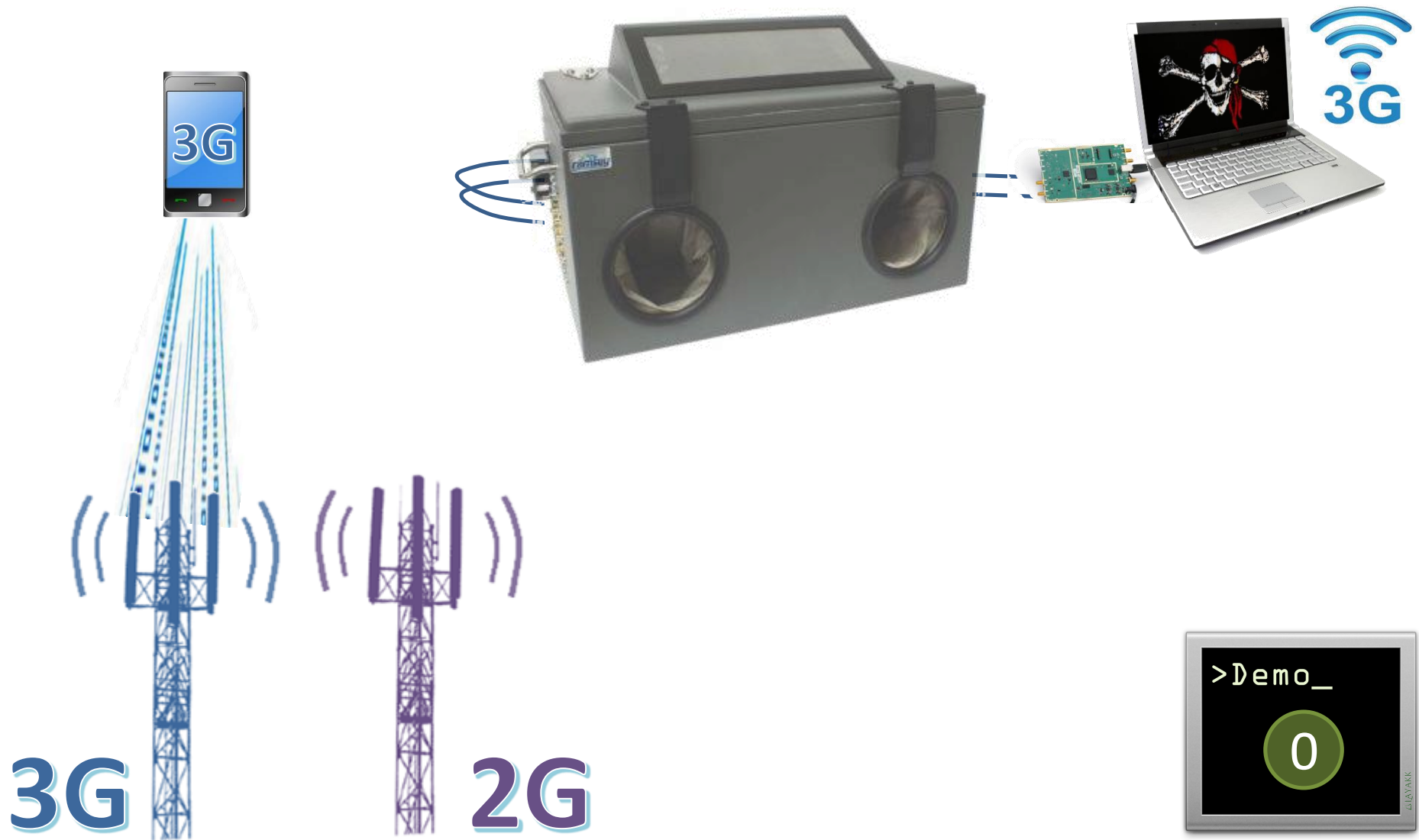
Downgrade selectivo a 2G



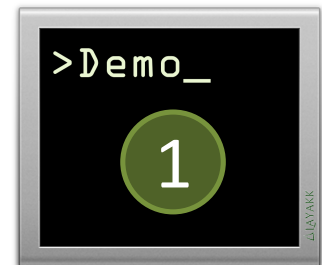
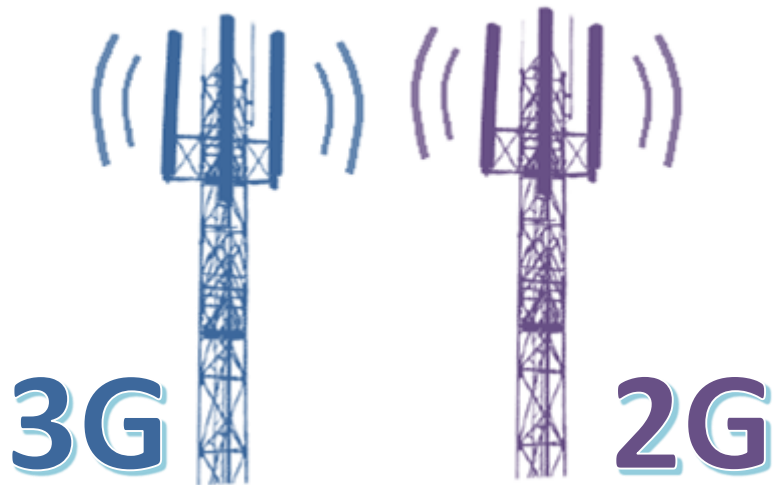
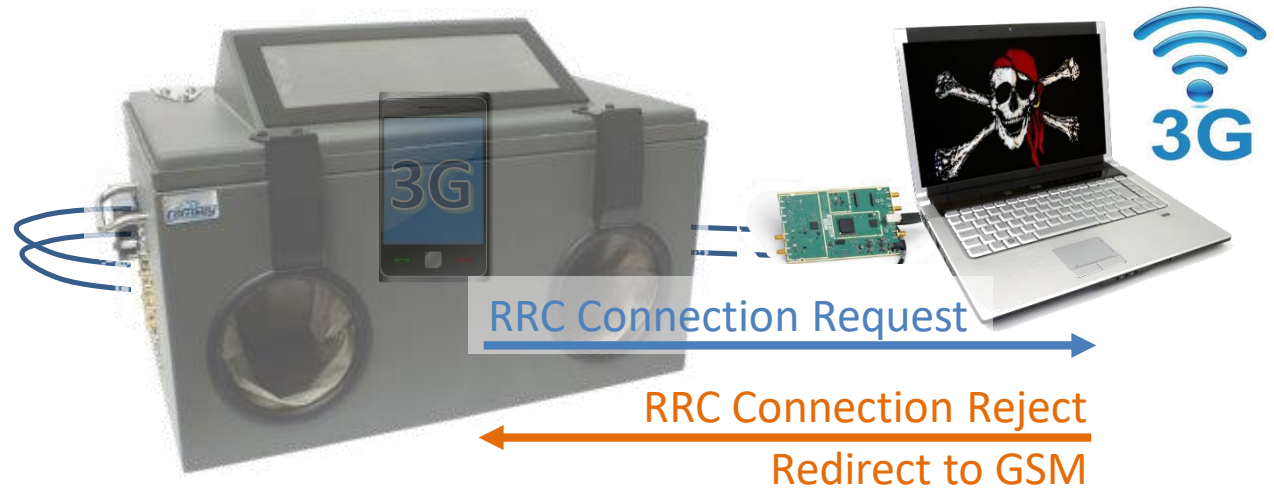
Downgrade a 2G



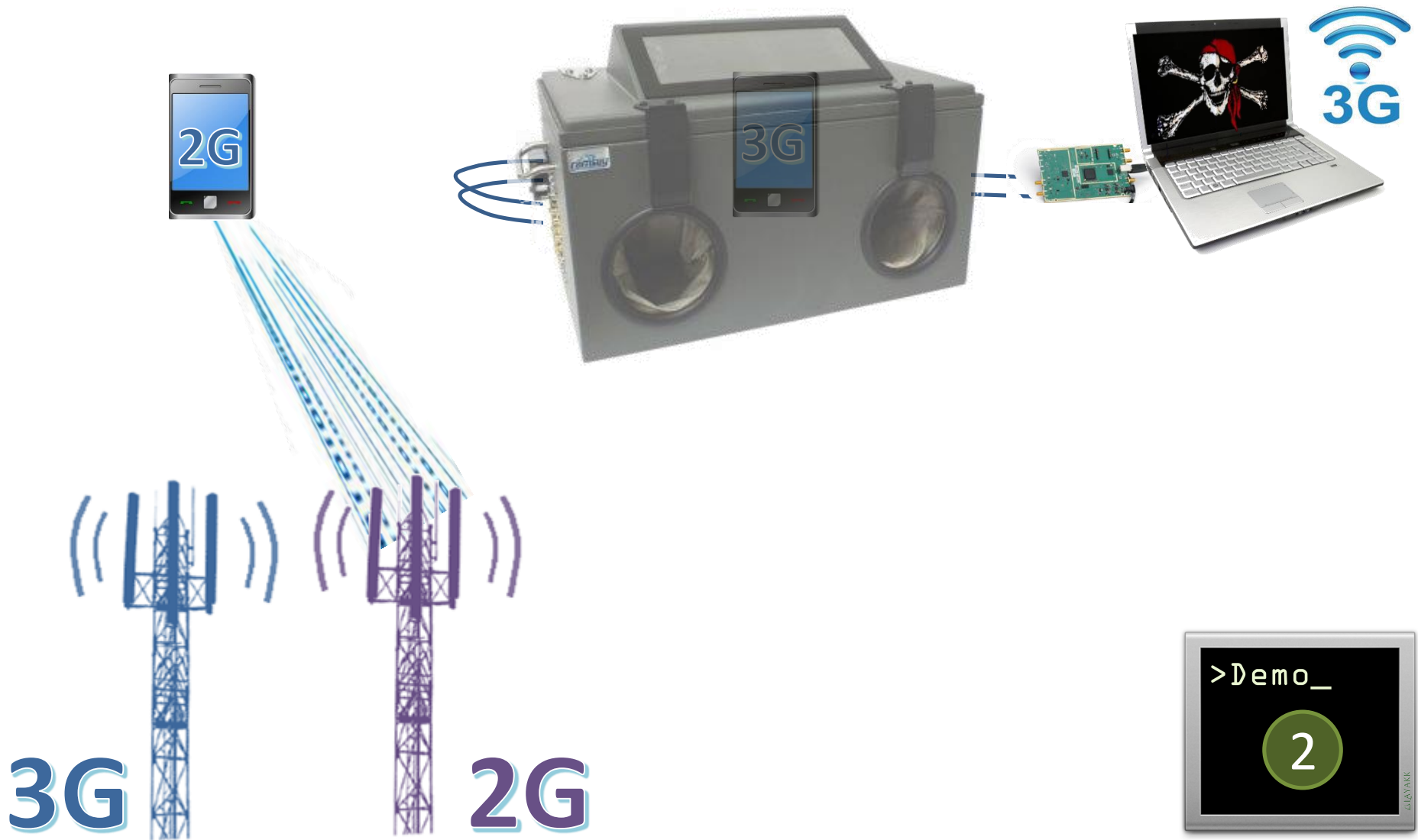
Downgrade a 2G



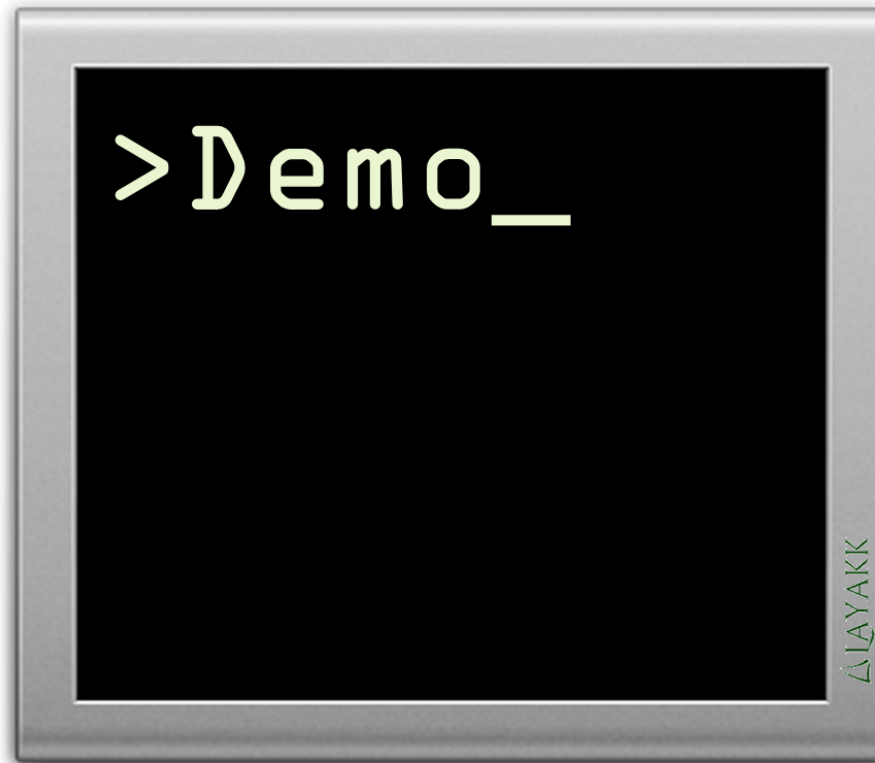
Downgrade a 2G



Downgrade a 2G



Downgrade a 2G



Downgrade selectivo a 2G

- Aunque se disponga de comunicaciones 3G, un atacante puede forzar las comunicaciones 2G del terminal víctima, lo que implica control completo de las mismas
 - Salvo que el terminal víctima esté configurado para no aceptar servicio 2G

Ataques 3G (estación base falsa)

- IMSI Catching es posible
- Geolocalización de dispositivos es posible
- Denegación de servicio persistente es posible
- Downgrade selectivo a 2G es posible

creemos que

Recomendaciones para usuarios y fabricantes

CONTRAMEDIDAS

Recomendaciones

Fabricantes
















- Posibilidad de deshabilitar el servicio 2G (y dejarlo deshabilitado por defecto)
- Aviso al usuario cuando el servicio es 2G,
 - especialmente si se fuerza a servicio no cifrado
- Aviso al usuario ante ciertos mensajes de señalización extremadamente infrecuentes:
 - Location Area / Routing Area Update Reject
 - [Illegal MS]
 - RRC Connection Reject
 - [Redirection]

Recomendaciones

Usuarios

- Desactivar el servicio 2G cuando sea posible
- Desplegar sistemas de detección de estaciones base falsas
- Solicitar y premiar a los fabricantes que implementen este tipo de medidas de protección en banda base

Recomendaciones

	Recomendación	IMSI Catching	Geolocalización	Denegación persistente	Downgrade Selectivo
Fabricantes	Opción Deshabilitar 2G				
	Aviso servicio 2G Aviso servicio no cifrado				
	Aviso mensajes señalización sospechosos				
Usuarios	Desactivar 2G				
	Desplegar sistemas de detección				
	Solicitar y premiar medidas de seguridad en banda base				

Aún tenemos temas pendientes



- Probar 4G

- Implicaciones eSIM

/Root@d[🔒] 2016

Atacando 3G vol. III



www.layakk.com
[@layakk](https://twitter.com/layakk)

José Picó
David Pérez

jose.pico@layakk.com
david.perez@layakk.com