



Hacking y Seguridad en Redes de Telefonía Móvil

Msc. Ing. Mauricio Canseco Torres



OWASP

The Open Web Application Security Project



OWASP

The Open Web Application Security Project

- Mauricio Canseco Torres
- Ing. de Sistemas – Ing. En Telecomunicaciones
- Msc. Seguridad en Internet
- Msc. Telefonía Móvil
- Especialista en seguridad para laCiberdefensa (Criptored)
- Hacker ético de Sistemas informáticos (Stack Overflow)
- Analista de Riesgos y Seguridad (ESR Proydesa)



OWASP

The Open Web Application Security Project

CONSIDERACIONES SOBRE EL HACKING Y SEGURIDAD EN REDES DE TELEFONÍA MÓVIL





OWASP

The Open Web Application Security Project

INTRODUCCIÓN

Powerful processors

Portability

Camera, GPS...

Email, app...

All conected over the air...(OTA)

Mobile is a game-changer in many ways...



OWASP

The Open Web Application Security Project

Crecimiento a gran escala...

- **>300,000** Mobile apps developed in three years (2007–2010)
- **\$1 billion** Mobile startup Instagram's value within 18 months
- **1.1 billion** Mobile banking (*m-banking*) customers by 2015
- **1.2 billion** Mobile broadband users in 2011
- **1.7 billion** Devices shipped in 2012 (an increase of 1.2 percent over 2011)
- **6 billion** Mobile subscriptions worldwide (China and India account for 30 percent)
- **\$35 billion** Estimated value of app downloads in 2014
- **76.9 billion** Estimated number of app downloads in 2014
- **\$1 trillion** Mobile payments (*m-payments*) estimated in 2015

- www.mobithinking.com



OWASP

The Open Web Application Security Project

Percepción de inseguridad...

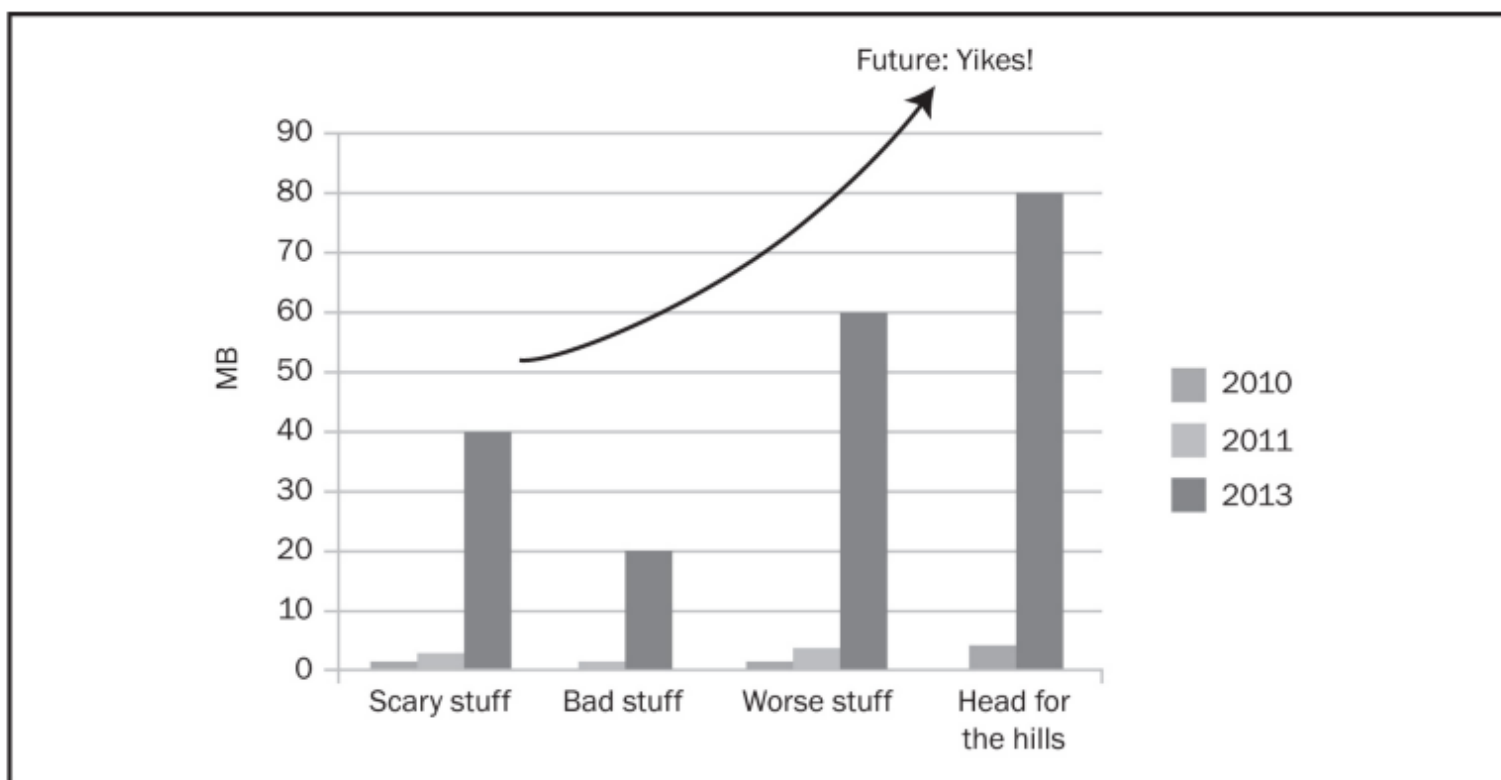
- McAfee's quarterly Threats Report indicated that mobile malware exploded 1,200 percent in the first quarter of 2012 over the last, or fourth, quarter of 2011.
- Trend Micro predicted 60 percent month-on-month malware growth on Android in 2012.
- IBM X-Force predicted that in 2011 "exploits targeting vulnerabilities that affect mobile operating systems will more than double from 2010."
- Apple's iOS had a greater than sixfold increase in "Code Execution" vulnerabilities, as tracked by CVE number, from 2011 to September 2012 (nearly 85 percent of the 2012 vulnerabilities were related to the WebKit open source web browser engine used by Apple's Safari browser).



OWASP

The Open Web Application Security Project

Percepción de inseguridad...



A typical mobile threat graph produced by industry

Modelo de Análisis de seguridad en Telefonía Móvil?

- Es bastante amplio...
- Complejo de definir..
- Convergencia de diversas tecnologías
- Es ambiguo... y genera confusión...



Confusión de conceptos...

Seguridad en Aplicaciones móviles

≠

Seguridad en S.O. móviles

≠

Seguridad en Redes de Telefonía móvil





OWASP

The Open Web Application Security Project

Seguridad en Aplicaciones Móviles





OWASP

The Open Web Application Security Project

Seguridad en S.O. Móviles



Seguridad en Redes Móviles

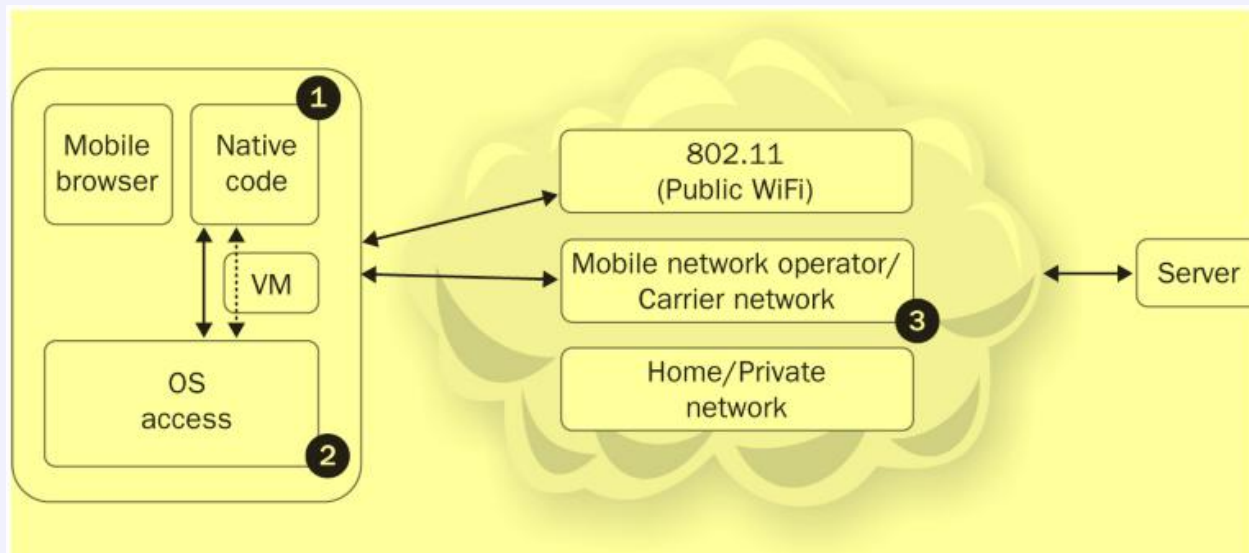
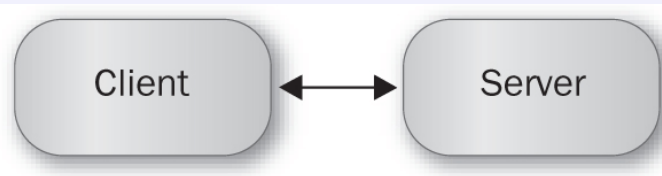




OWASP

The Open Web Application Security Project

Alternativa de análisis, una Arquitectura cliente Servidor...





OWASP

The Open Web Application Security Project

Definiendo un Modelo de Riesgos para el ecosistema de Telefonía Móvil

- Los StackeHolders:
 - Operadores de Red Móvil
 - Fabricantes de Dispositivos
 - “Vendors” de S.O. móviles (Google, Apple, etc)
 - Tiendas de Aplicaciones
 - Empresas de TI.
 - Desarrolladores de aplicaciones móviles
 - Usuarios Finales



OWASP

The Open Web Application Security Project

Operadores de Red Móvil



OWASP



Fabricantes de dispositivos móviles

- <http://celulares.about.com/od/Smartphones/tp/Principales-Fabricantes-De-Telefonos-Celulares-En-El-Mundo.htm>



OWASP

The Open Web Application Security Project

Fabricantes de Sistemas operativos



Google



Firefox OS



BlackBerry



OWASP

The Open Web Application Security Project



Android Market

An open content distribution system that will help end users find, purchase, download and install various types of content on their Android-powered devices.



iPhone App Store

An online market for applications, called "App Store". It is a service for the iPhone, iPod Touch, and now the iPad. By using this app store, iPhone users can download any app they want through iTunes or directly from their phones to take advantage of all available iPhone features.



Ovi Store

Ovi Store is a service where customers can download mobile games, applications, videos, images, and ringtones to their Nokia devices. Some of the items are free, others can be purchased using a credit card or through operator billing for selected operators.



BB App World

BlackBerry App World is an application distribution service from Research In Motion (RIM) for most BlackBerry devices. The service provides BlackBerry users with an environment to browse, download, and update third-party applications.



Windows Phone Marketplace

Windows Phone Marketplace is a service from Microsoft for its Windows Phone 7 platform that allows users to browse and download applications that have been developed by third parties.

Tiendas de aplicaciones móviles

Empresas de TI



OWASP

The Open Source Security Project



TOSHIBA

acer



AOC
EYES VALUE



SanDisk

ISB BOLA BASIC
EALASTROS Y REGULADORES

SONY

APC
Legendary Reliability™

ASUS

lenovo



Acteck

BenQ
Enjoyment Matters

iomega

LEXMARK

Kensington
smart made simple

Canon

EPSON
EXCEED YOUR VISION



Kingston
TECHNOLOGY

Genius

TRIPP-LITE
POWER PROTECTION



WD Western Digital

LINKSYS
A Division of Cisco Systems, Inc.

SMC
Networks

COMPLET
ENERGIA CONFIABLE

D-Link
Building Networks for People



OWASP

The Open Web Application Security Project



Desarrolladores de App. Móviles



OWASP

The Open Web Application Security Project

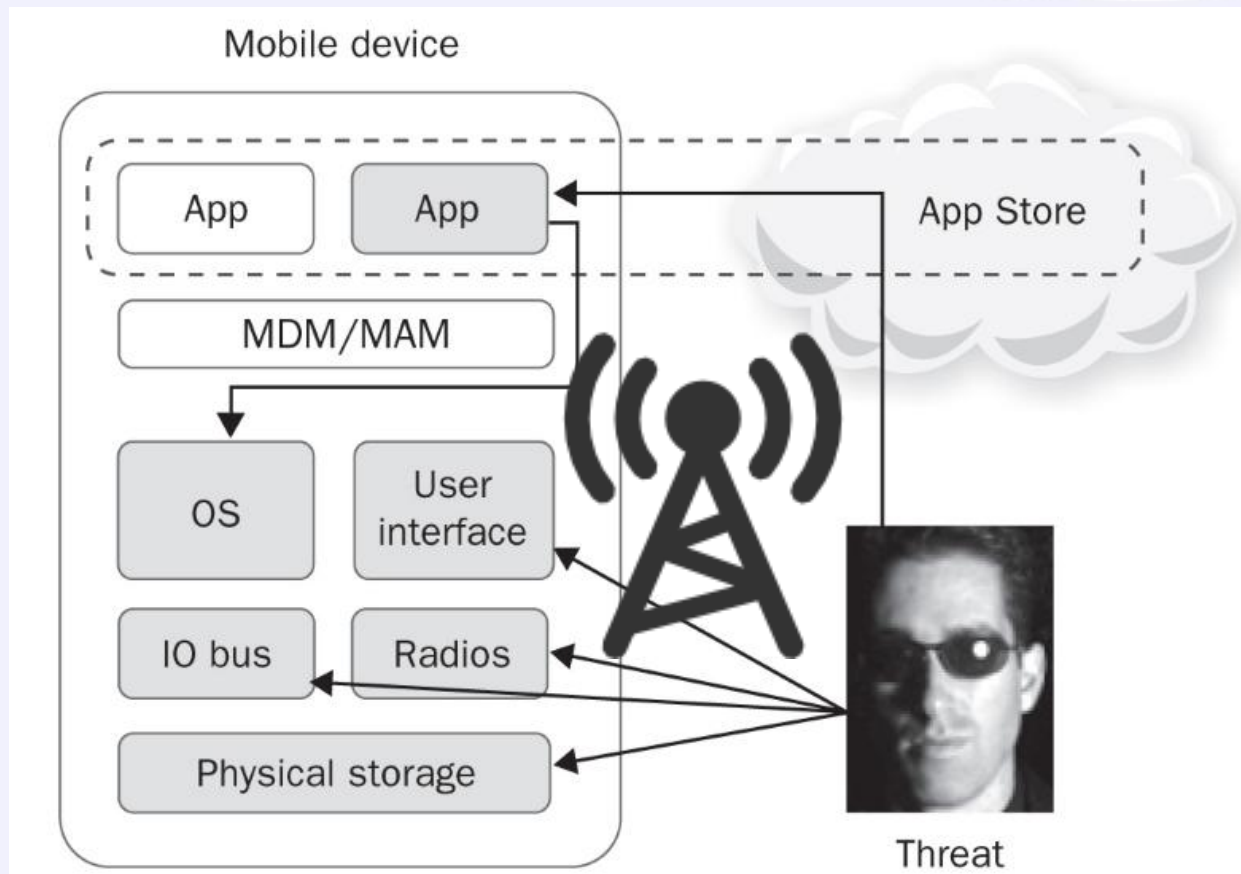


Usuarios Finales



OWASP

The Open Web Application Security Project



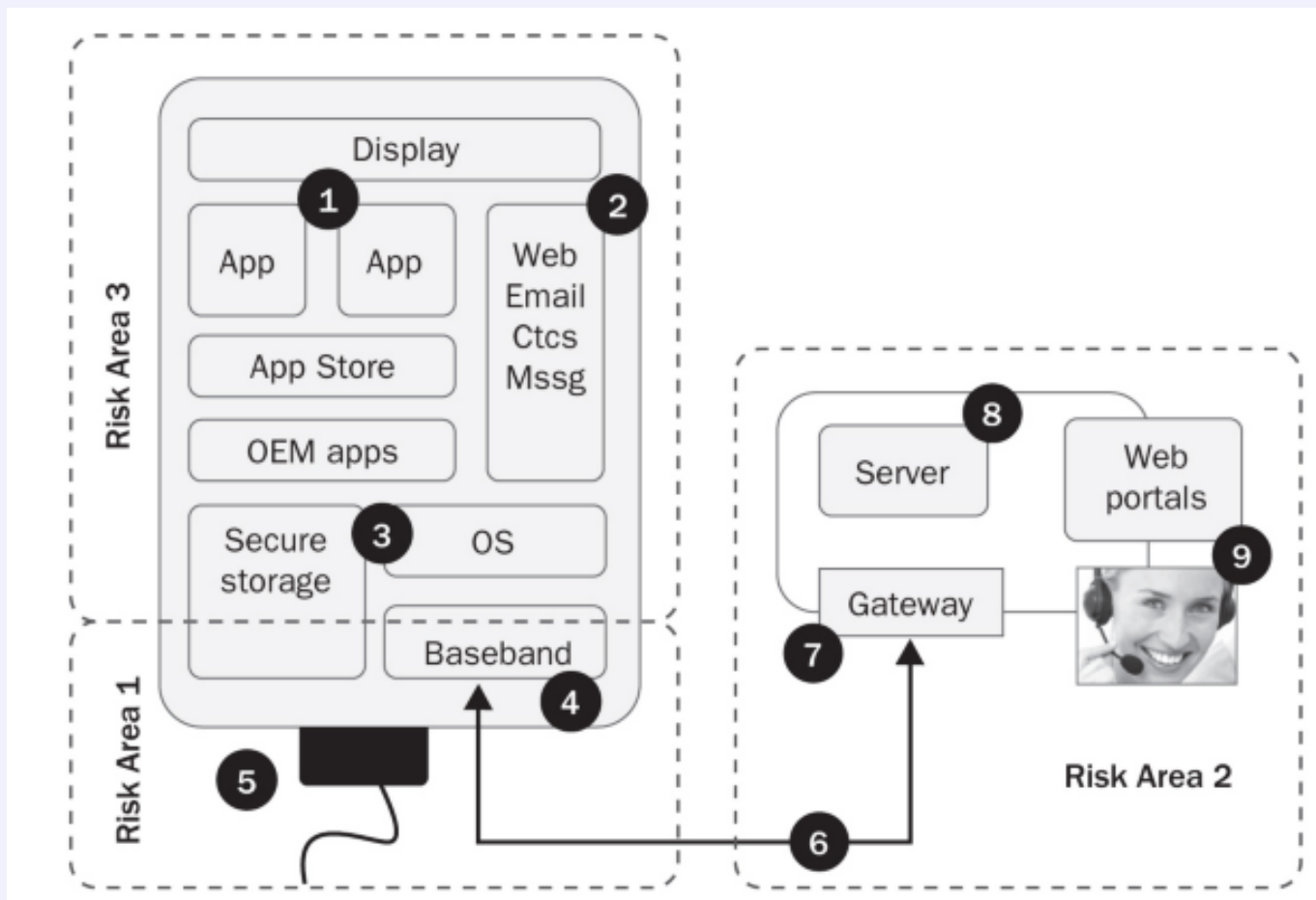
Hacking Exposed Mobile: Security Secrets & Solutions 1st Edition



OWASP

The Open Web Application Security Project

Modelo Genérico de Riesgos...





OWASP

The Open Web Application Security Project

Seguridad en Redes de Telefonía Móvil, Una propuesta de análisis de su seguridad

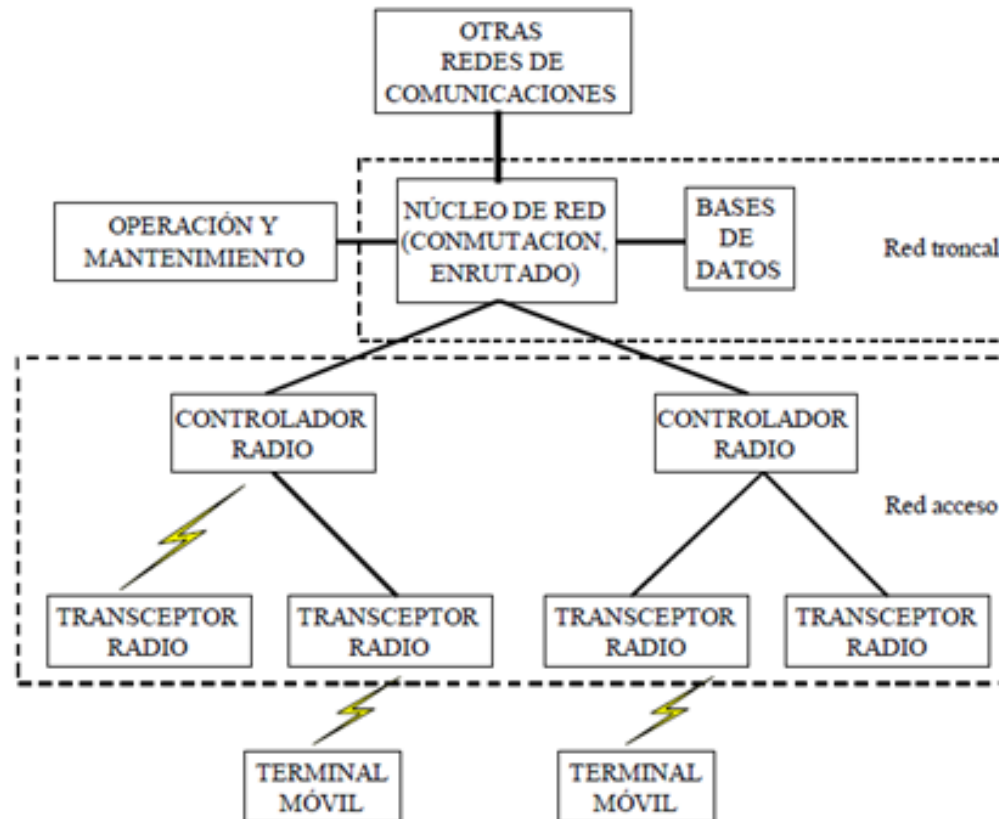
- Su estudio e importancia se ha incrementado en los últimos años.
- Una red de telefonía Móvil sin importar la generación móvil a la que pertenezca, por fines de simplicidad para el análisis de la seguridad, estará conformado por:
 - Arquitectura estructural
 - Esquema de dominios operacionales



OWASP

The Open Web Application Security Project

Arquitectura Genérica de una Red Celular



Arquitectura Genérica de una Red Celular

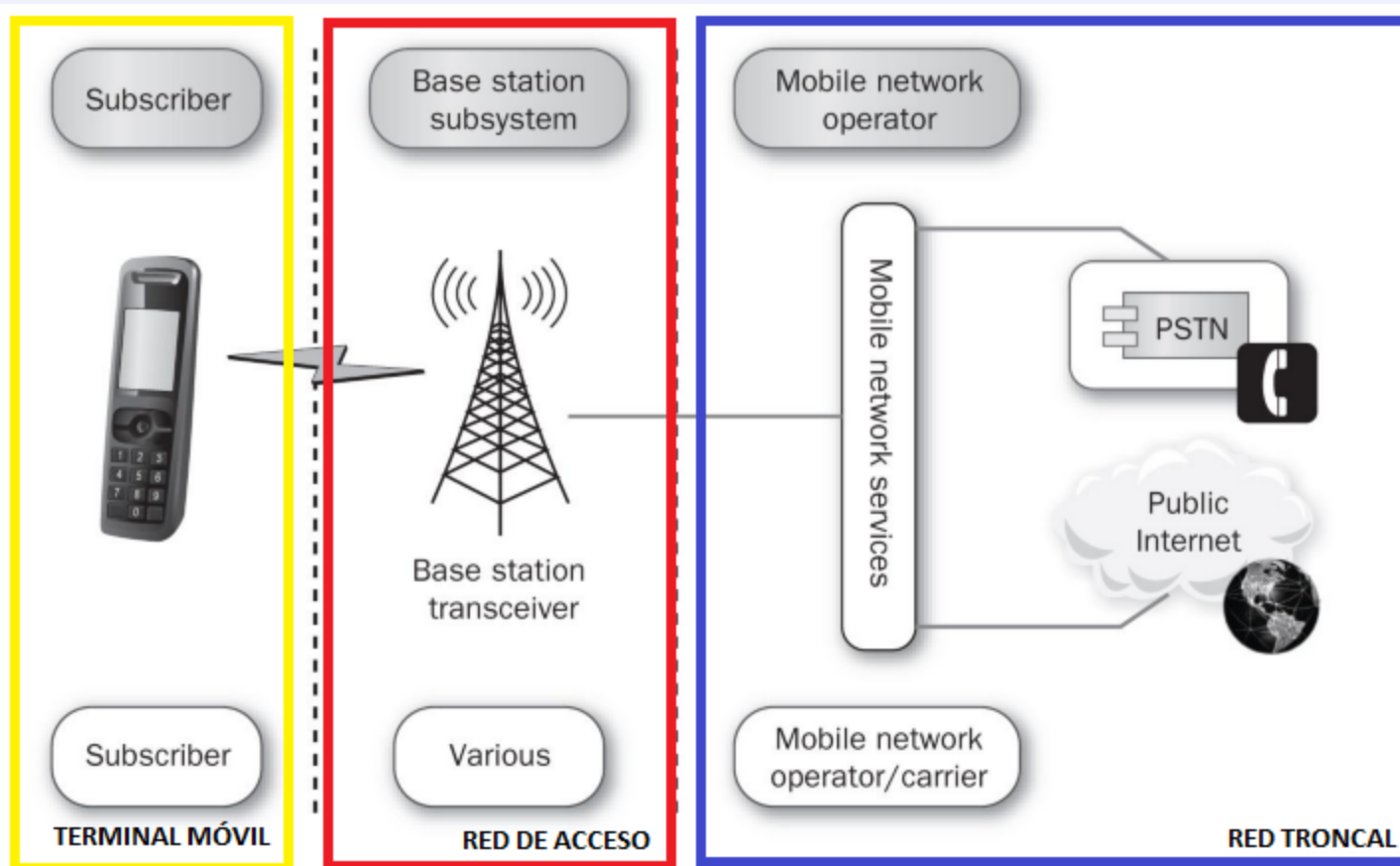
Fuente: "Principios de Comunicaciones Móviles", (Sallent, Valenzuela, & Agustí, 2003)



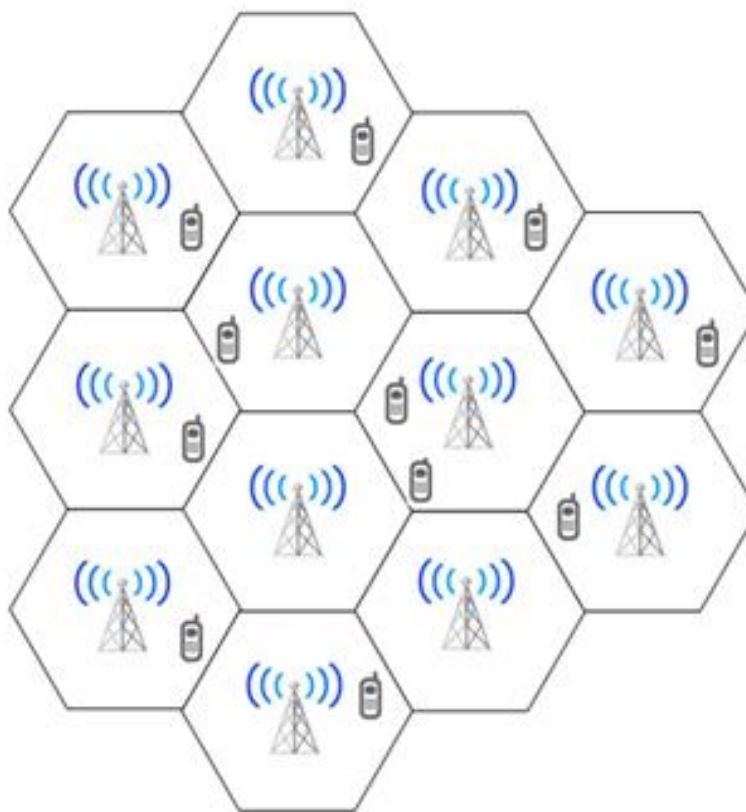
OWASP

The Open Web Application Security Project

Arquitectura Simplificada de una Red Celular



La Red de Acceso, una red celular...



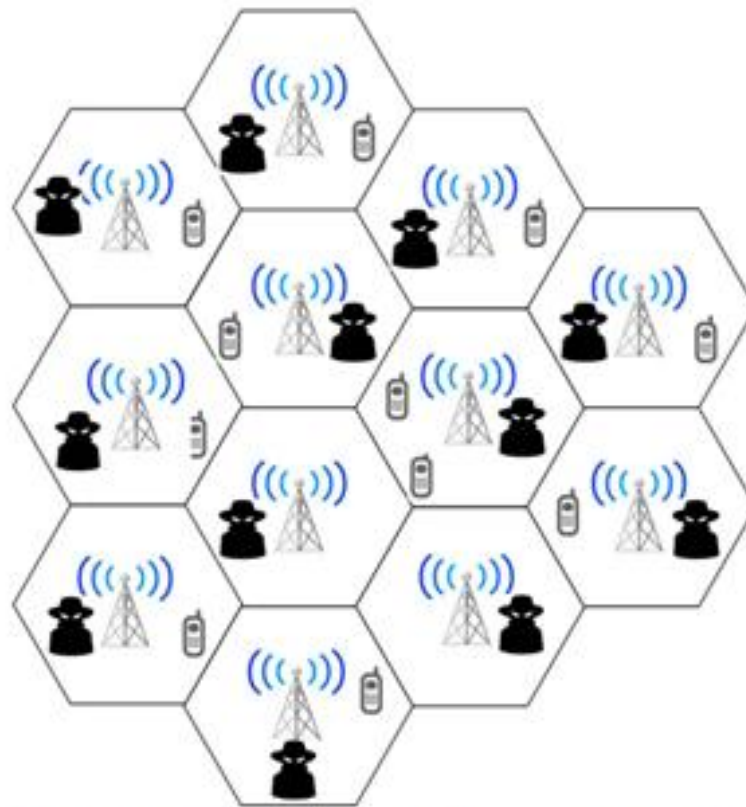
Esquema básico de distribución celular de una Red Móvil



OWASP

The Open Web Application Security Project

Red Celular desde el punto de vista del atacante

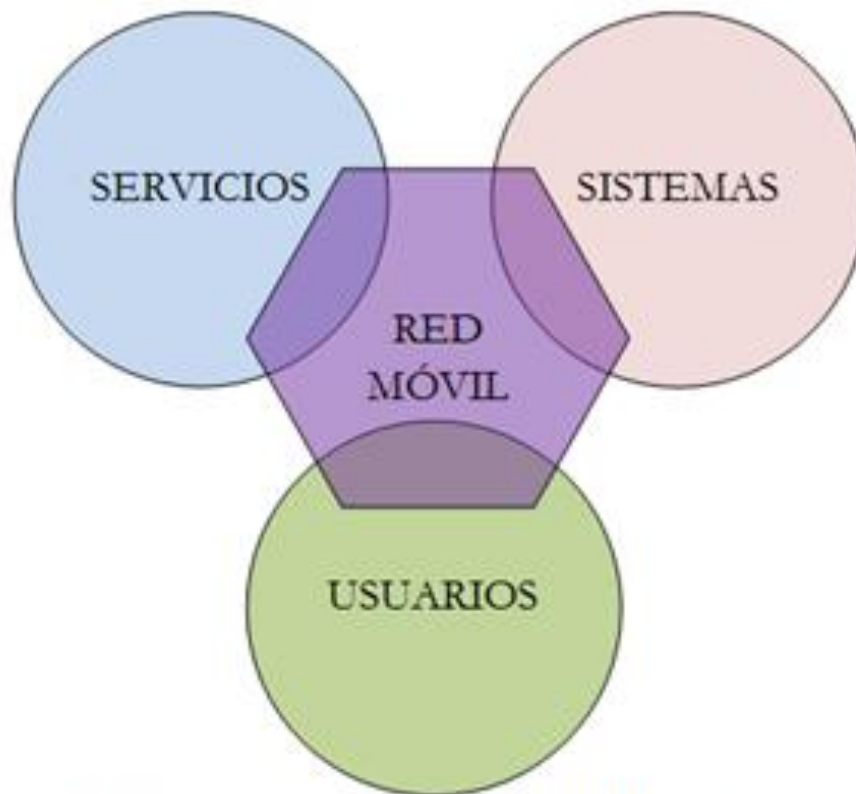


Perspectiva de la distribución celular de una Red Móvil para un Atacante



OWASP

The Open Web Application Security Project

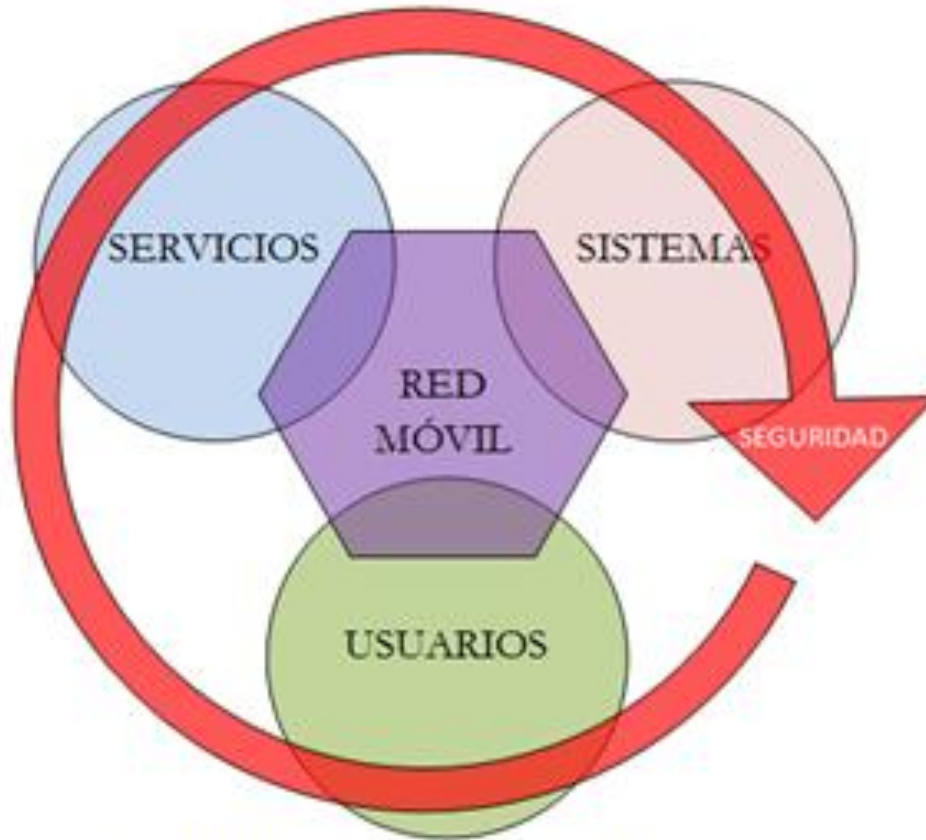


Dominios Operacionales del Core de una Operadora Móvil desplegados a través de la Red

Esquema de Dominios Operacionales



OWASP
The Open Web Application Security Project



Seguridad en una Red de Telefonía móvil

Seguridad sobre los Dominios Operacionales



OWASP

The Open Web Application Security Project



CORE DE UNA OPERADORA DE TELEFONÍA MÓVIL



OWASP

The Open Web Application Security Project

2G	VOZ		
	DATOS		
3G	VOZ y DATOS		
	4G	VOZ y DATOS	

ACTUAL TECNOLOGÍA MÓVIL



OWASP

The Open Web Application Security Project

Tecnología	Generación
AMPS	1G
TACS	1G
GSM	2G
CDMA	2G
GPRS	2.5G
EDGE	3G
WiMAX/LTE	4G

Tecnologías de Telefonía Móvil

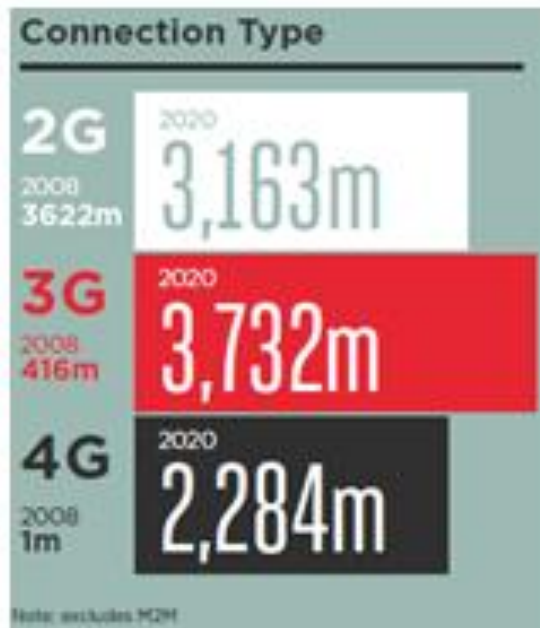
Fuente: "*Certified Ethical Hacker (CEH) CErt Guide*", (Gregg, 2014)

Sobre la Generación Móvil



OWASP

The Open Web Application Security Project



Tipo de conexiones año 2008 vs. 2020.

Fuente: "Mobile Economy 2014". (GSMA, 2014)

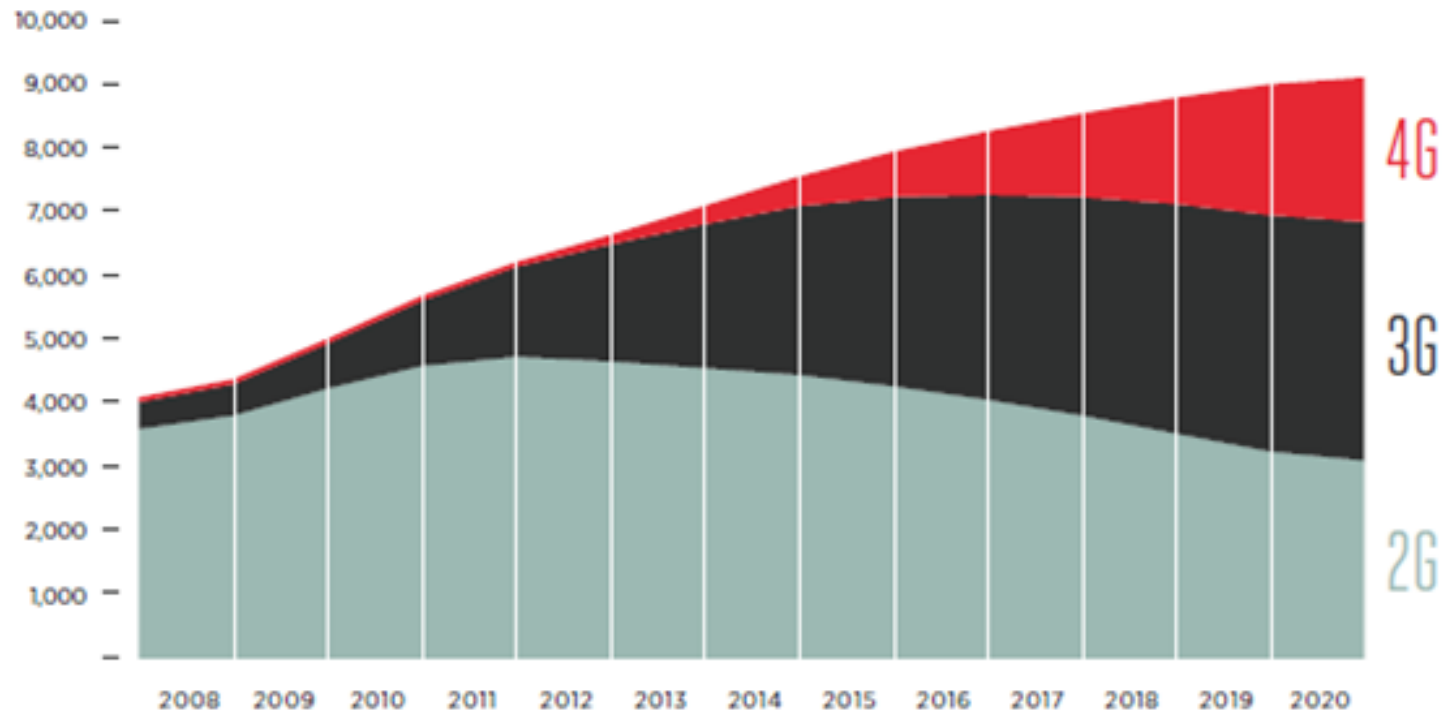
Sobre la Generación Móvil



OWASP

Global connections by technology

(m, ex-M2M)



Conexiones Globales por tecnología.

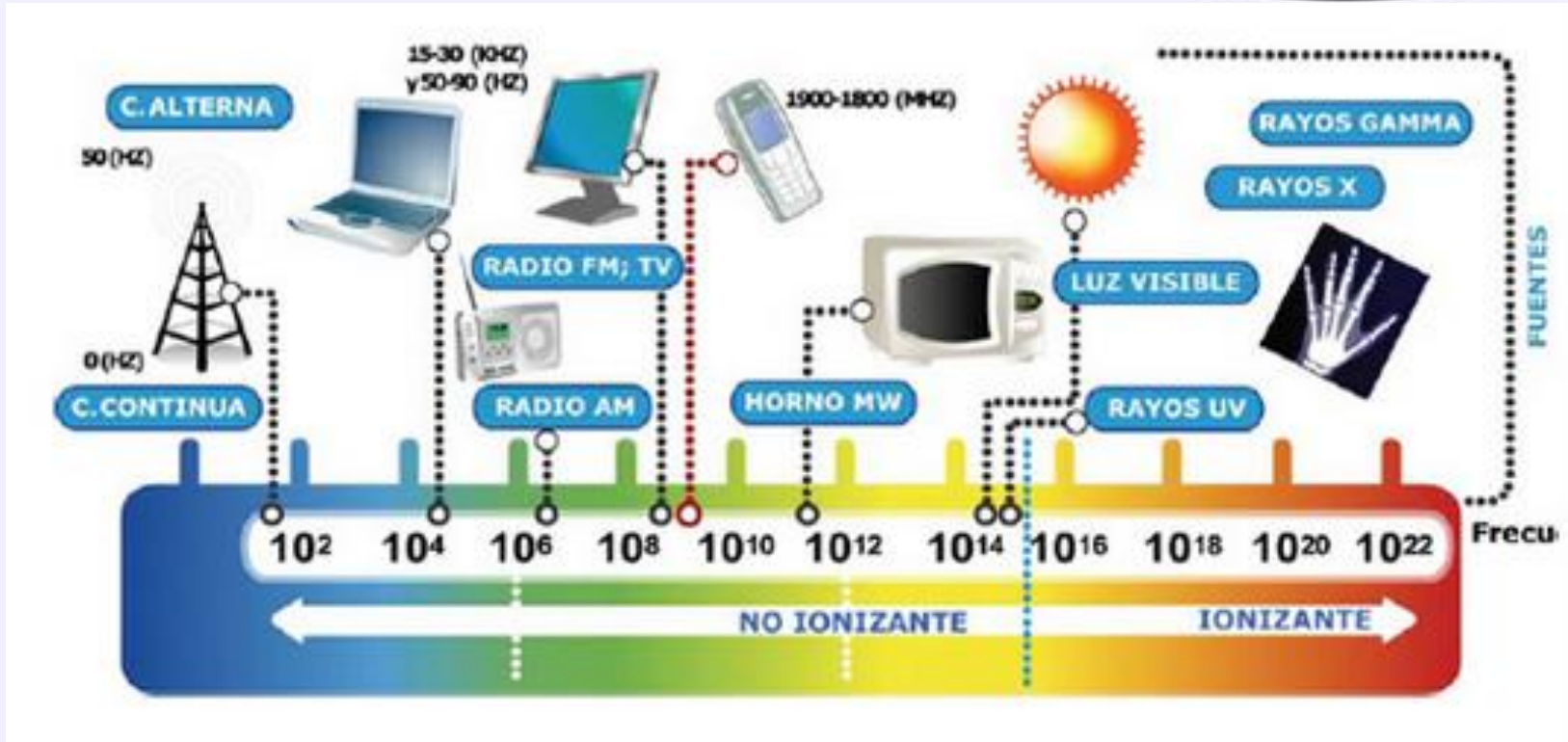
Fuente: "Mobile Economy 2014". (GSMA, 2014)

Sobre la Generación Móvil



OWASP

The Open Web Application Security Project

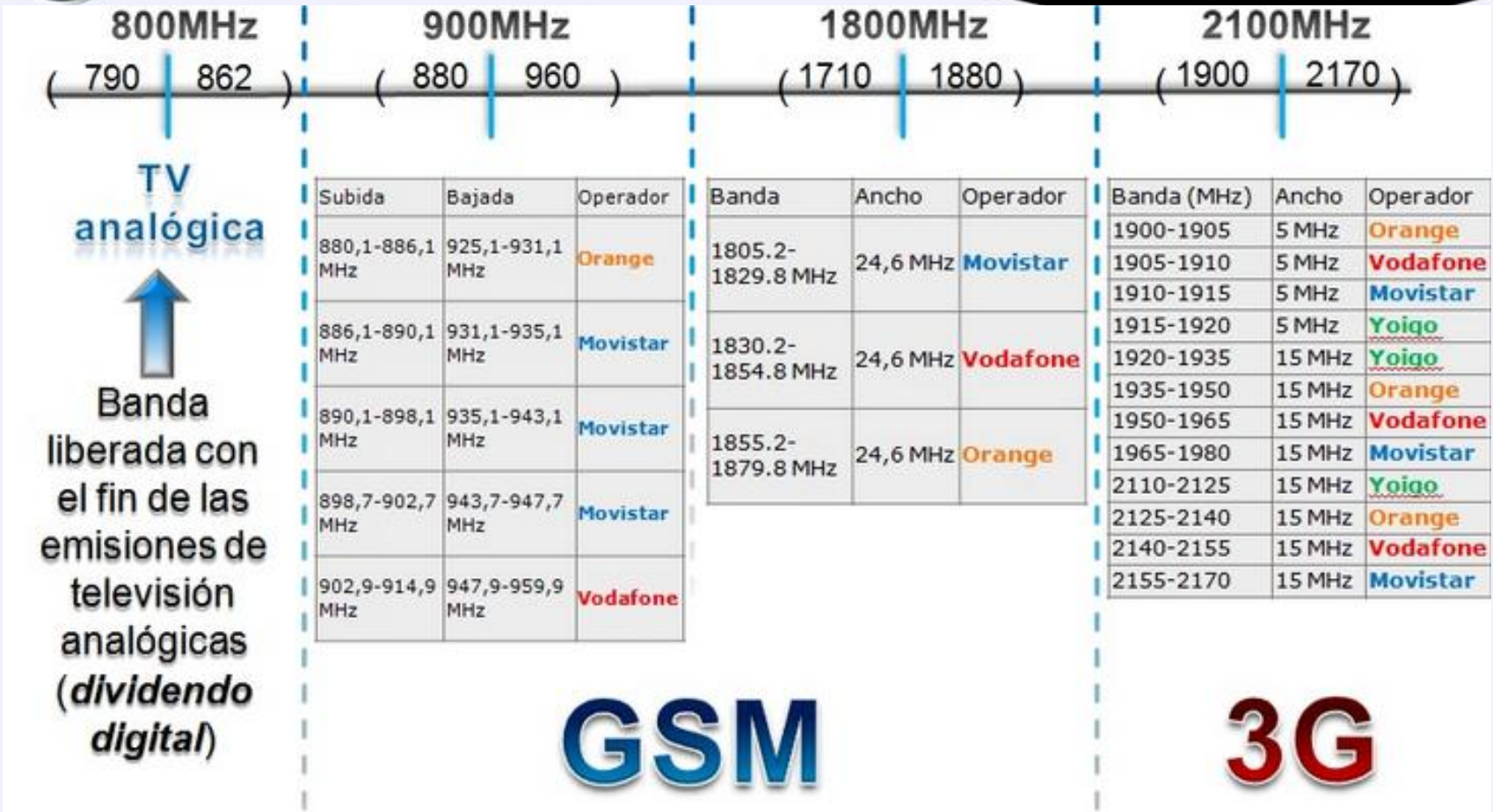


El espectro electromagnético y la telefonía móvil



OWASP

The Open Web Application Security Project



Frecuencias de Operación por Generación Móvil



OWASP

The Open Web Application Security Project



- La comunicación analógica
- La voz viajaba en claro, simplemente modulada en frecuencia

1G: Primeros estándares de “telefonía Móvil”



OWASP

The Open Web Application Security Project

- AMPS (Advanced Mobile Phone System) operaba en la banda de 800 MHz. América, África, Europa del Este y Rusia.
- ETACS (Extended Total Access Communications System). Europa, y utilizaba la banda de 900MHz.
- NMT (Nordic Mobile Telephone) países escandinavos en la banda de 900 MHz.



1G: Primeros estándares de “telefonía Móvil”



OWASP

The Open Web Application Security Project



No hay seguridad en esta tierra, sólo hay
oportunidad.

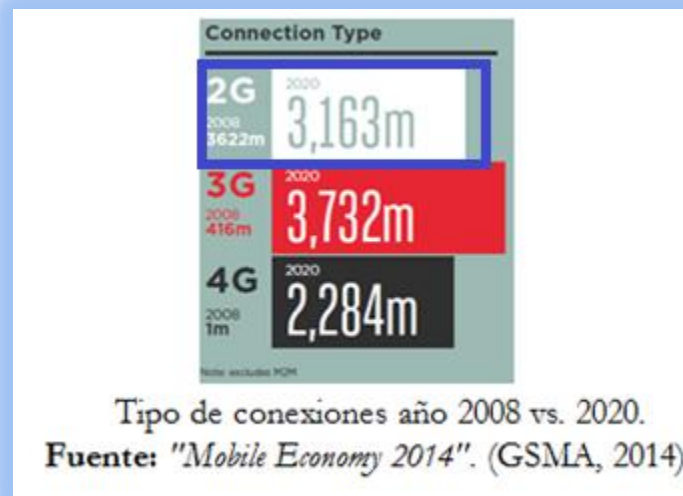
(Douglas MacArthur)

1G: Seguridad



OWASP

The Open Web Application Security Project



2G: Comunicaciones de voz



OWASP

The Open Web Application Security Project

SEGURIDAD EN GSM

- ✓ Sistema celular digital
- ✓ Modulación GMSK
- ✓ Conmutación de circuitos
- ✓ Canales de voz a 13 Kbps
- ✓ Mínimas capacidades de datos:
- ✓ 9,6 Kbps por circuito de datos (CSD)

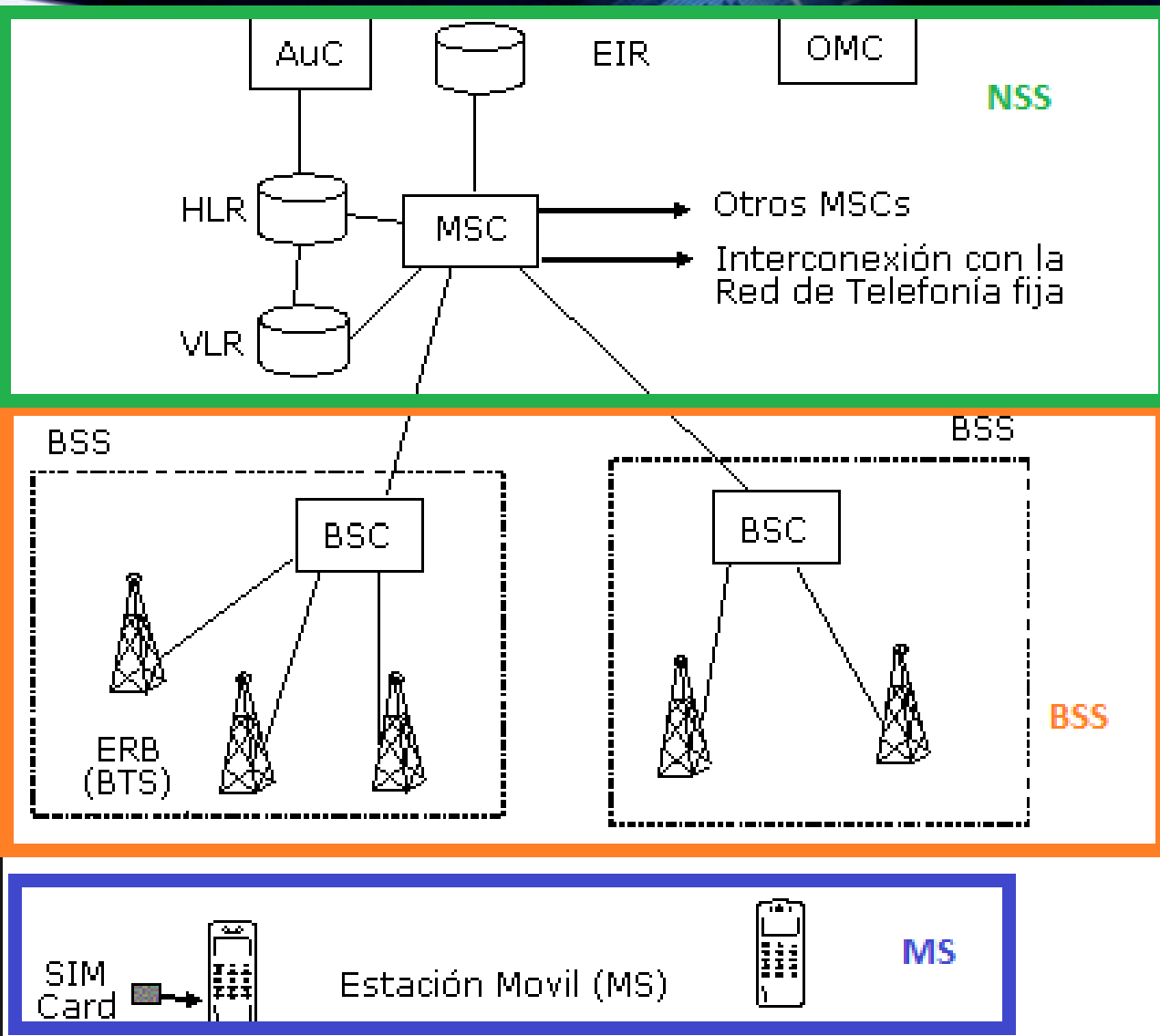
Características Generales



OWASP

The Open Web Application Security Project

GSM



Arquitectura de GSM



OWASP

The Open Web Application Security Project

- Formado Básicamente por dos elementos

- ME (Mobile Equipment)



Caracterizado por IMEI

(International Mobile Equipment Identifier)

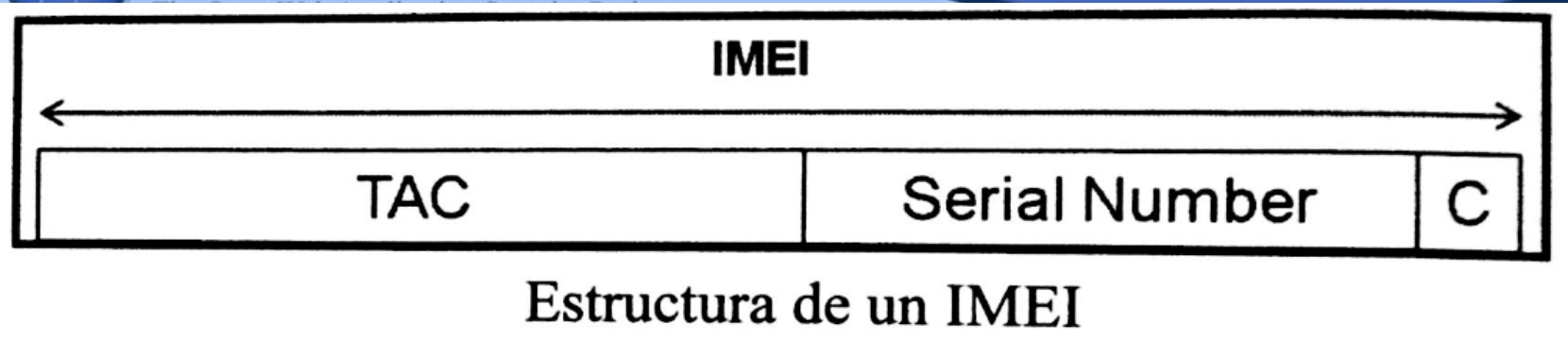
- SIM (Subscriber Identity Module)



Caracterizado por IMSI y el Ki

(International Mobile Subscriber Identity)

MS (Mobile Station)



TAC-Type Allocation Code (2+6=8 dígitos)

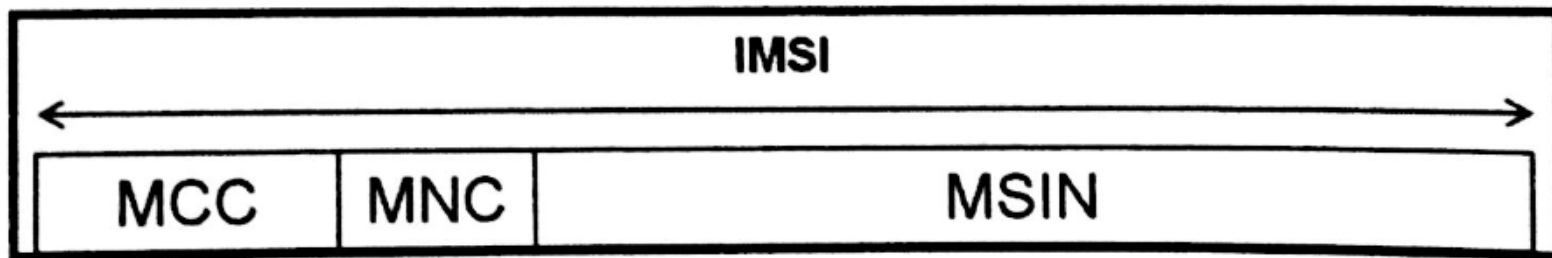
Serial Number (6dígitos)

Checksum (1 dígito)

IMEI



IMSI



Estructura de un IMSI (*International Mobile Subscriber Identity*)

MCC-Mobile Country Code (3 dígitos)

MNC- Mobile Network Code (2 dígitos Eu, 3 USA)

MCC	MNC	Bolivia		
736	01	Viva Bolivia	Operativa	GSM 1900
736	02	Entel Bolivia	Operativa	GSM 850 / GSM 1900
736	03	Telecel Bolivia	Operativa	GSM 850

MSIN- Mobile Station Identification Number (8 o 9)



- Confidencialidad del suscriptor (HSSD)
- Autenticación del suscriptor
- Confidencialidad en comunicaciones de señalización y de usuario.

Aspectos de Seguridad en GSM

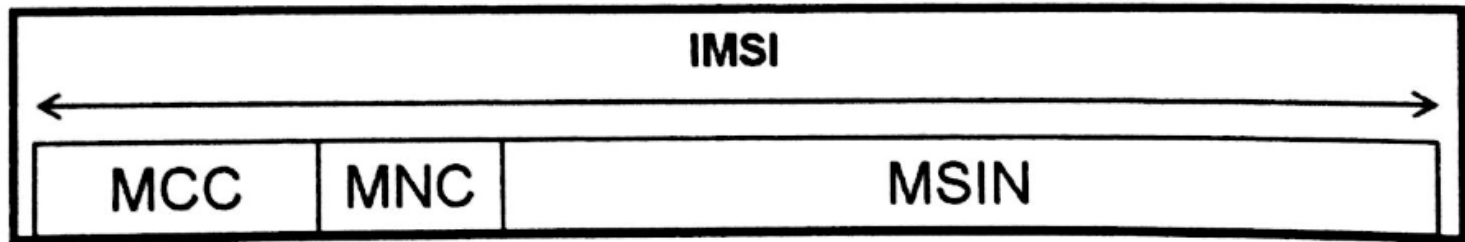




OWASP

The Open Web Application Security Project

• Autenticación mediante el IMSI



Estructura de un IMSI (*International Mobile Subscriber Identity*)

- IMSI, considerado por la norma como información sensible... (Delata la ubicación del usuario...)

Autenticación GSM: Identificación del Usuario en la Red




OWASP

The Open Web Application Security Project



Mobile Network Explorer

TELÉFONO MÓVIL RED CELULAR SERVICIOS



Operador de Red:	73602
Nombre del Operador:	Movil GSM
Tipo de Red:	HSPA
Country ISO:	bo
IMSI:	73602 [redacted] 9
Roaming:	No
IccCard:	Si

IMSI muy confidencial???

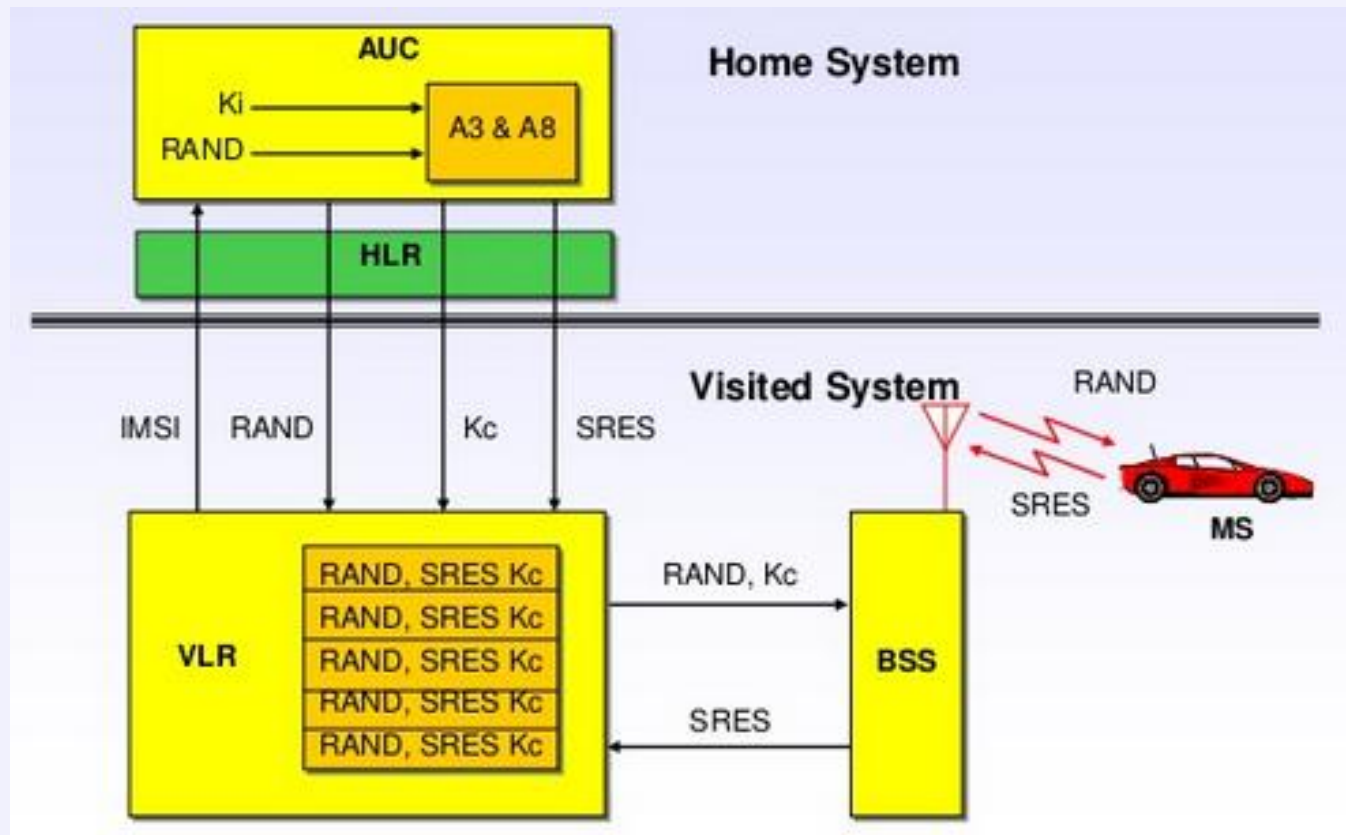


OWASP

The Open Web Application Security Project

Proceso de autenticación y generación de clave de sesión

- **Ki**
- **Kc**
- **RAND**
- **SRES**



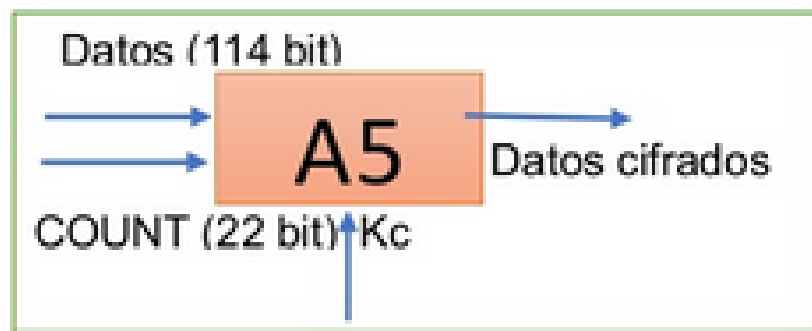
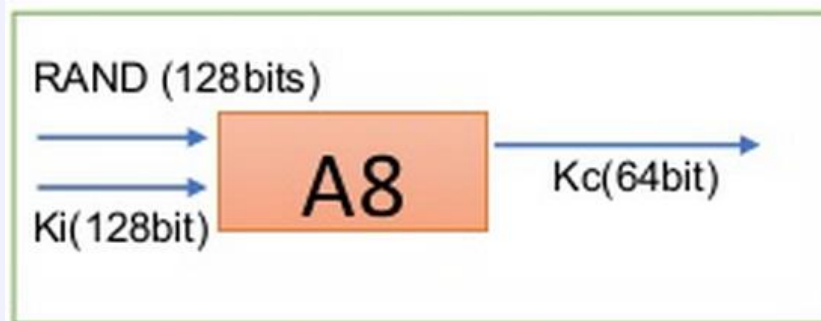
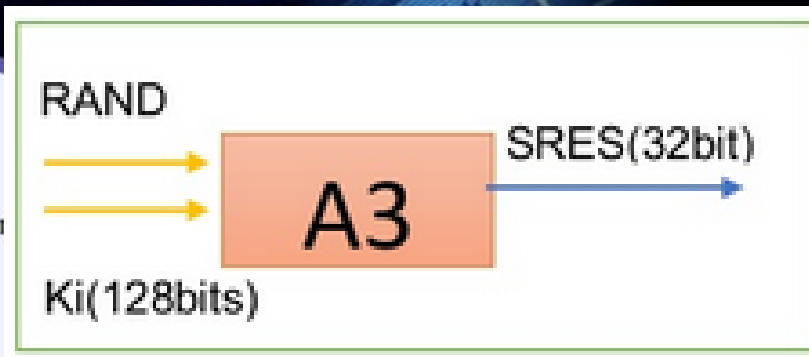


OWASP

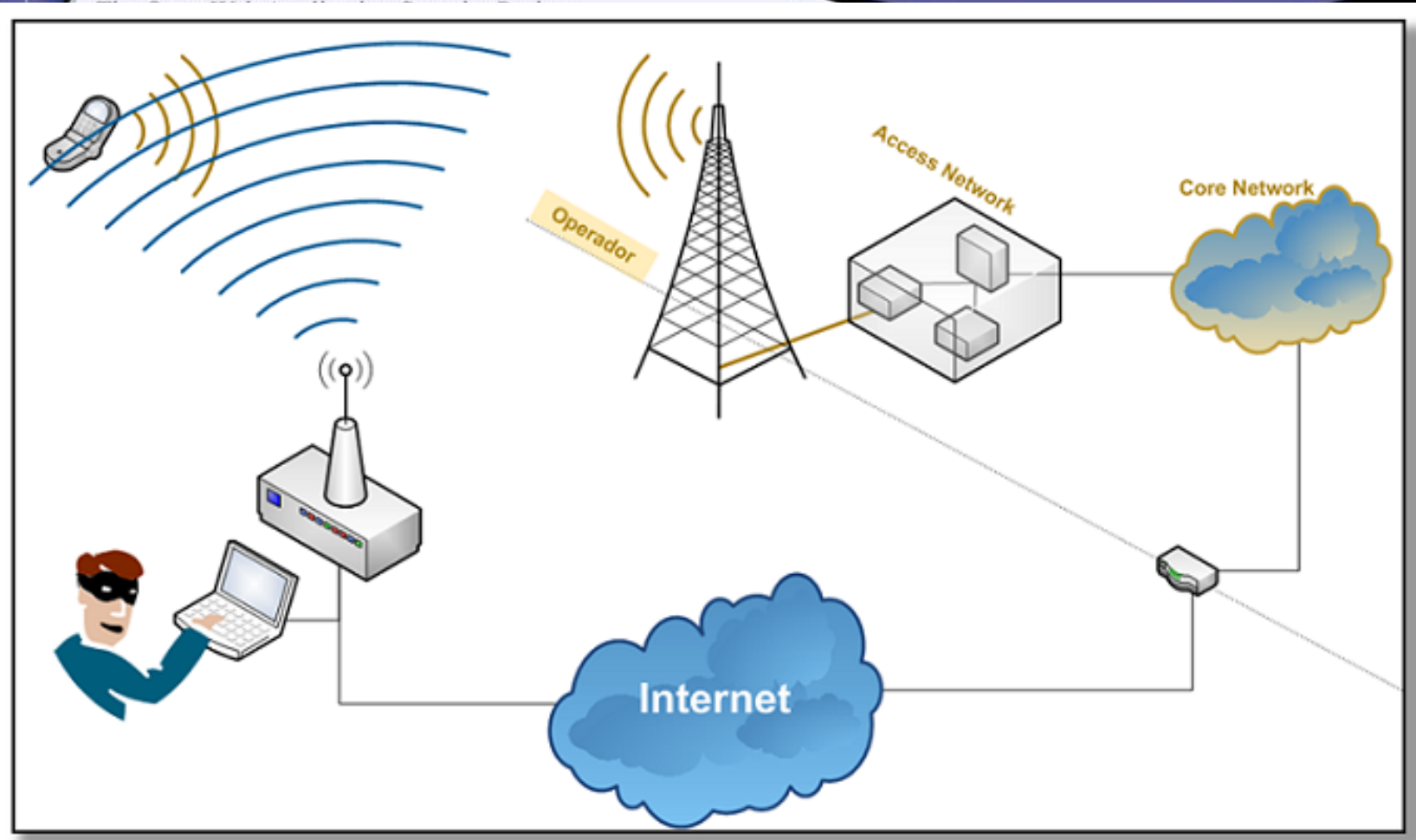
The Open Web Application Security Project

- GSM cifra, a partir de un momento en la comunicación, la voz y los datos de señalización.
- Normalmente el cifrado se realiza con el algoritmo A5/1
 - El algoritmo A5/1 es un algoritmo que genera un bitstream por cada unidad de transmisión (ráfaga).
 - El bitstream se combina (XOR) con la ráfaga a transmitir
 - La generación del bitstream depende de una clave de sesión y del número de trama TDMA.

Cifrado de las comunicaciones GSM



Algoritmos Criptográficos GSM



Infiltración en la red del operador



OWASP

The Open Web Application Security Project

- IMSI revela la ubicación de un usuario
- La norma sugiere el uso de A5/0 como método de cifrado.
- Debilidades de los algoritmos de cifrado.
- MS no autentica la red.
- La obtención de Kc solo depende de RAND y Ki.



Ataques contra comunicaciones GSM



OWASP

The Open Web Application Security Project



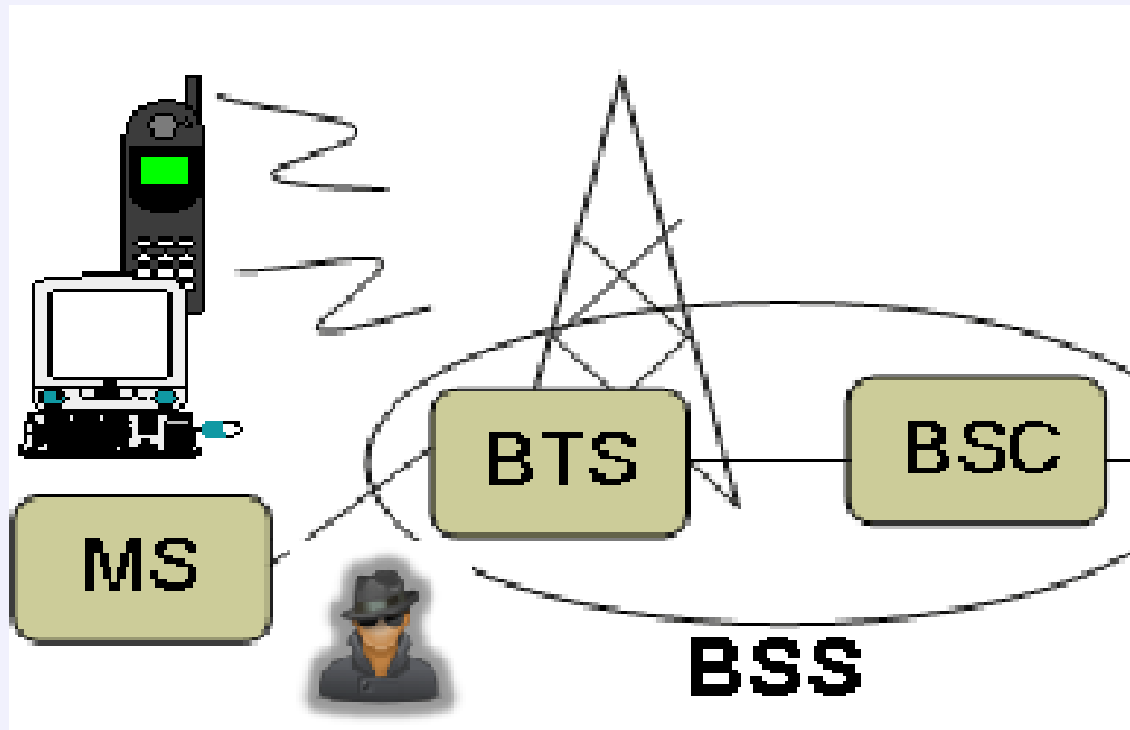
Infiltración en la red del operador



OWASP

The Open Web Application Security Project

- El punto de escucha es el interfaz radio entre la estación base y la MS.



Escucha del canal de Radio (Señalización)



OWASP

The Open Web Application Security Project

- Recuperar información sobre la red (fingerprinting)
- Recuperar información sobre un usuario (Presencia en la red, generación de tráfico o localización geográfica)

Escucha del canal de Radio (Señalización)



OWASP

The Open Web Application Security Project

Equipo y software necesario

- Equipo Radio (USRP + tarjeta RA900 MHz, teléfono OsmocommBB o dispositivos basados en Realtek TRL283U)



OWASP

The Open Web Application Security Project

- USRP



USRP X310- \$5,520.00 USD

783145-01 | KINTEX7-410T FPGA, 2 CHANNELS, 10 GIGE AND PCIE BUS

The Ettus Research USRP X310 is a high-performance, scalable software platform for designing and deploying next generation wireless communication systems. The hardware architecture combines two extended-bandwidth daughterboards, DC - 6 GHz with up to 120 MHz of baseband bandwidth, multiple high-speed interfaces (PCIe, dual 10 GigE, dual 1 GigE), and a large user-programmable FPGA. It is available in a convenient desktop or rack-mountable half-wide 1U form factor. In

- <http://fakebts.com/uhd-usrp/>
- <http://www.ettus.com/>

Relativamente caro...!!



OWASP

The Open Web Application Security Project

- Teléfono OsmocommBB



Motorola . C115 . Super Oferta . Outlet

\$ 85⁰⁰

12 cuotas de \$ 10⁸⁴

- <http://bb.osmocom.org/trac/wiki/MotorolaC123>
- <http://fakebts.com/osmocom/>

Alternativa Económica



OWASP



osmocomBB

wiki: [Hardware](#) / [Phones](#)

Following is a list of hardware that is supported by OsmocomBB or work-in-progress. The individual implementations.

TI Calypso based

Information specific to certain [Hardware/Calypso/Rita/Iota](#) based phones that we support

- Designed + Manufactured by Compal, OEM by Motorola
 - [MotorolaC115/C117](#) (E87)
 - [MotorolaC123/C121/C118](#) (E88) -- our primary target
 - [MotorolaC140/C139](#) (E86)
 - [MotorolaC155](#) (E99) -- our secondary target
 - [MotorolaV171](#) (E68/E69)
 - [SonyEricssonJ100i](#)
- Designed by Pirelli/Foxconn?, manufactured by Foxconn
 - [Pirelli DP-L10](#)
- Designed by Openmoko, manufactured by FIC
 - Neo 1973 (GTA01)
 - [OpenMoko](#) - Neo Freerunner (GTA02)



OWASP

The Open Web Application Security Project

- Radio demodulador de señal GSM
- GNU radio + airprobe



- <http://gnuradio.org/>
- <http://www.dragonjar.org/airprobe-instalacion-y-uso.xhtml>

Equipo y software necesario



OWASP

The Open Web Application Security Project

- Decodificador de los canales de control común de GSM
- Airprobe + Wireshark



- <https://www.wireshark.org/>
- <https://svn.berlin.ccc.de/projects/airprobe/>



OWASP

The Open Web Application Security Project

- Implementación de algoritmos de frequency hopping
- Técnicas de criptoanálisis de algoritmos de cifrado (A5 Security project)



OWASP

The Open Web Application Security Project

Posibilidad de realización del ataque?

- Hasta hace un par de años con dificultad.
(Frequency hopping y cifrado)
- Chipset RealTek RTL2832U.
- Proyecto OsmoSDR
- Ubicación entre MS y BTS es crítica.

Escucha del Canal de radio (Datos)

- Similar al ataque anterior.
- El atacante puede grabar la comunicación y descubrir Kc mediante alguna técnica criptográfica.

Equipo.- Similar al anterior, adicionalmente

- Técnicas de criptoanálisis de A5
- Técnicas de decodificación de los códigos de voz de GSM (OpenBTS + asterisk)





OWASP

The Open Web Application Security Project

Confidencialidad en las comunicaciones??

- Ki – Clave precompartida entre el usuario y la red, de la que se deriva la clave de sesión con la que se cifran las comunicaciones: Kc
- Las comunicaciones se cifran normalmente con el algoritmo A5/1
- Los móviles están obligados a aceptar el modo de cifrado que les indique el operador, incluyendo A5/0 (no cifrado)



OWASP

The Open Web Application Security Project

Ataques de Suplantación de usuarios

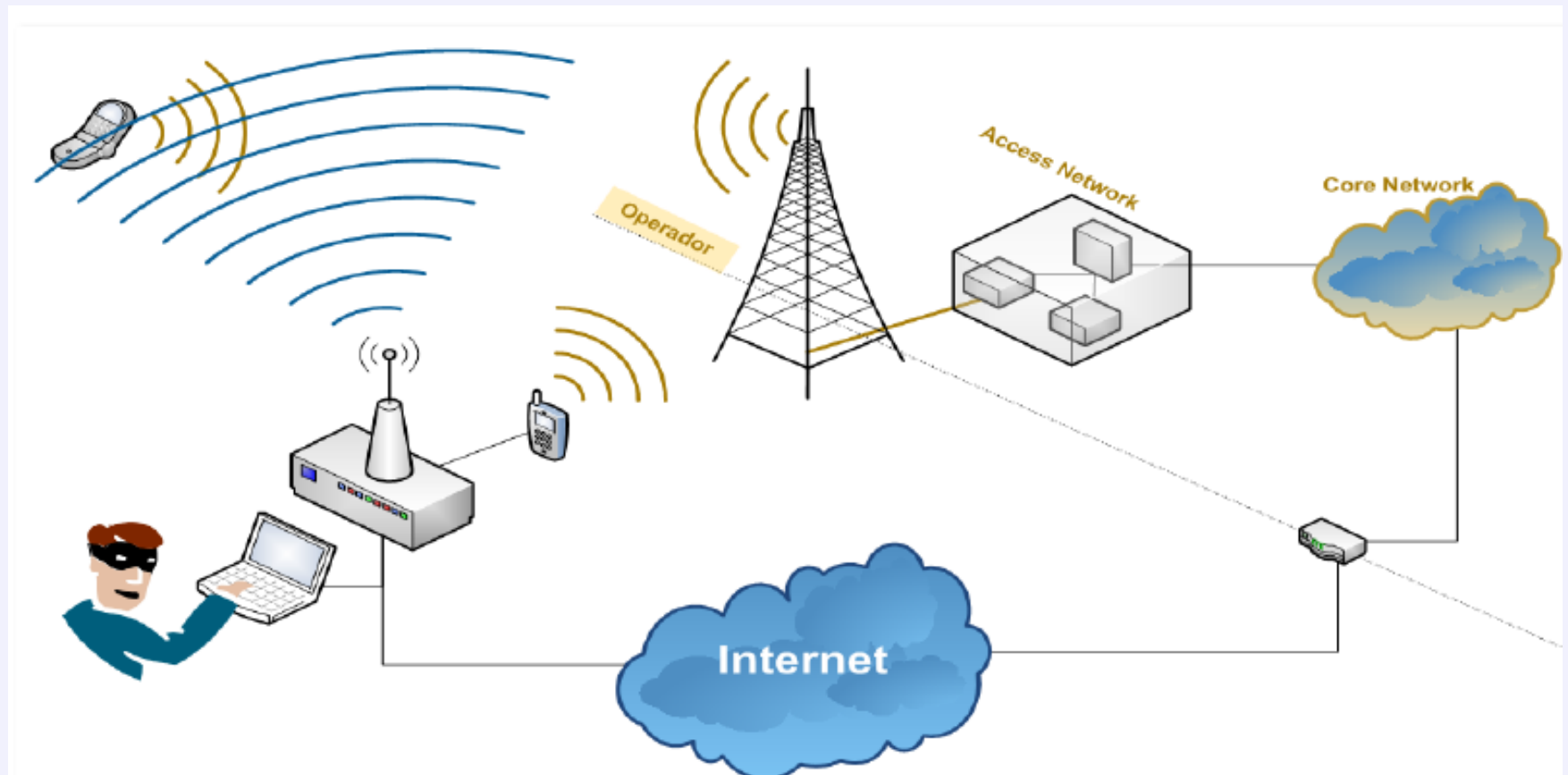
- Parte del hecho de que:
 - Un atacante puede obtener Kc.
 - El atacante puede capturar el TMSI asociado a la víctima.
 - Usando un Segundo teléfono OsmocommBB el atacante inserta TMSI y Kc... Se autentica en la red...!!!



OWASP

The Open Web Application Security Project

Suplantación de Usuarios..





OWASP

The Open Web Application Security Project

Ataques mediante Estación Base Falsa

- En primera instancia, el atacante caracteriza el espacio radioeléctrico.

▶ kal

▶ tadschan

▶ Field Test Mode

▶ OsmocommBB





OWASP

The Open Web Application Security Project

Puede suplantarse al operador??

- No hay autenticación de red, pero se necesitaría:
- Conocer la(s) frecuencia(s) en uso del espacio radioeléctrico de la zona.
- Conocer la(s) celda(s) que “posiblemente” está dando servicio al móvil víctima.
- Conocer, para cada una de esa(s) celda(s), sus identificativos, sus frecuencias y la lista de celdas declaradas como vecinas
- Conseguir que la víctima perciba más potencia de la estación falsa que de la legítima



Método

Paso inicial

- Caracterización de Espacio Radioeléctrico
- PLMN (Operador)
- IMSI



Paso 1

- Frecuencia de emisión
- Códigos de identificación del operador
- Parámetros de la red
- Potencia de señal



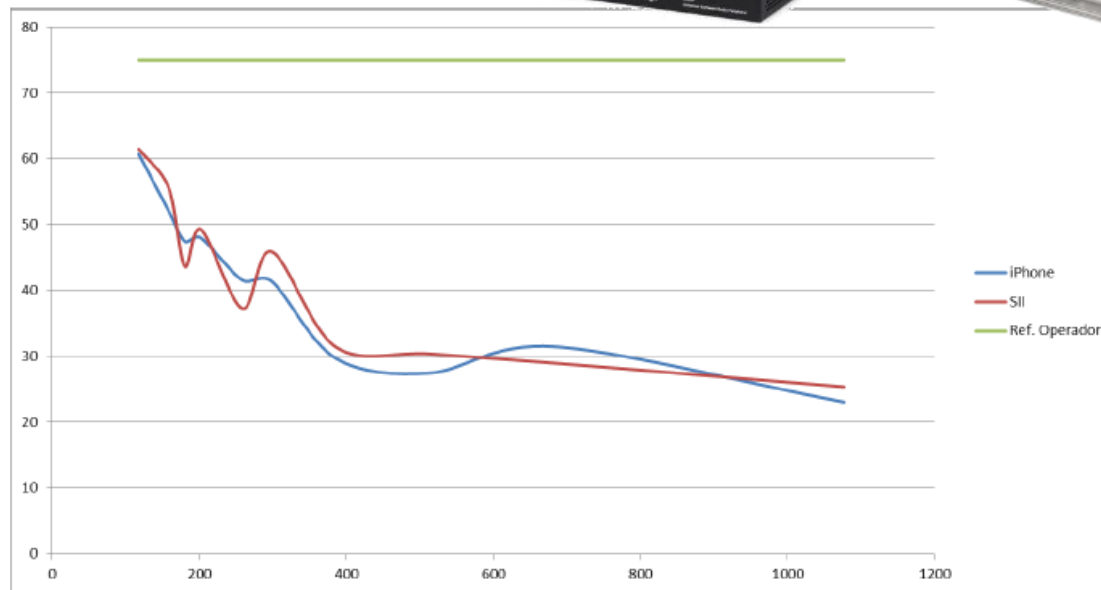
OWASP

The Open Web Application Security Project



Sobre la potencia de señal...

Potencia de emisión



Método



OWASP

The Open Web Application Security Project



Paso 2:emisión

- Inhibir ARFCN ó
- Suplantar a una de las celdas
(CRO - Cell Reselection Offset)



Paso 2:emisión

- La señal debe tener los parámetros adecuados en su beacon:
- Mismo MCC y NCC
- Un ARFCN legítimo
- Una LAI diferente de la celda vecina
- Nivel de potencia adecuado



Paso 3: aceptación del registro

- Obtener IMSI y el IMEI
- La estación base fuerza usar el algoritmo A5/0

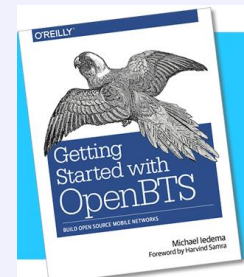
Equipamiento



OWASP

The Open Web Application Security Project

- Hardware capaz de emitir en banda de GSM (USRP + GNU RADIO)
- MÓDEM GMSK
- OPEN BTS (Open Source Cellular infraestructure)
<http://openbts.org/>
- Central de conmutación *asterisk*
<http://www.asterisk.org/>
- Software de captura de señal GSM (airprobe)





OWASP

The Open Web Application Security Project

Equipo principal.... OJO...



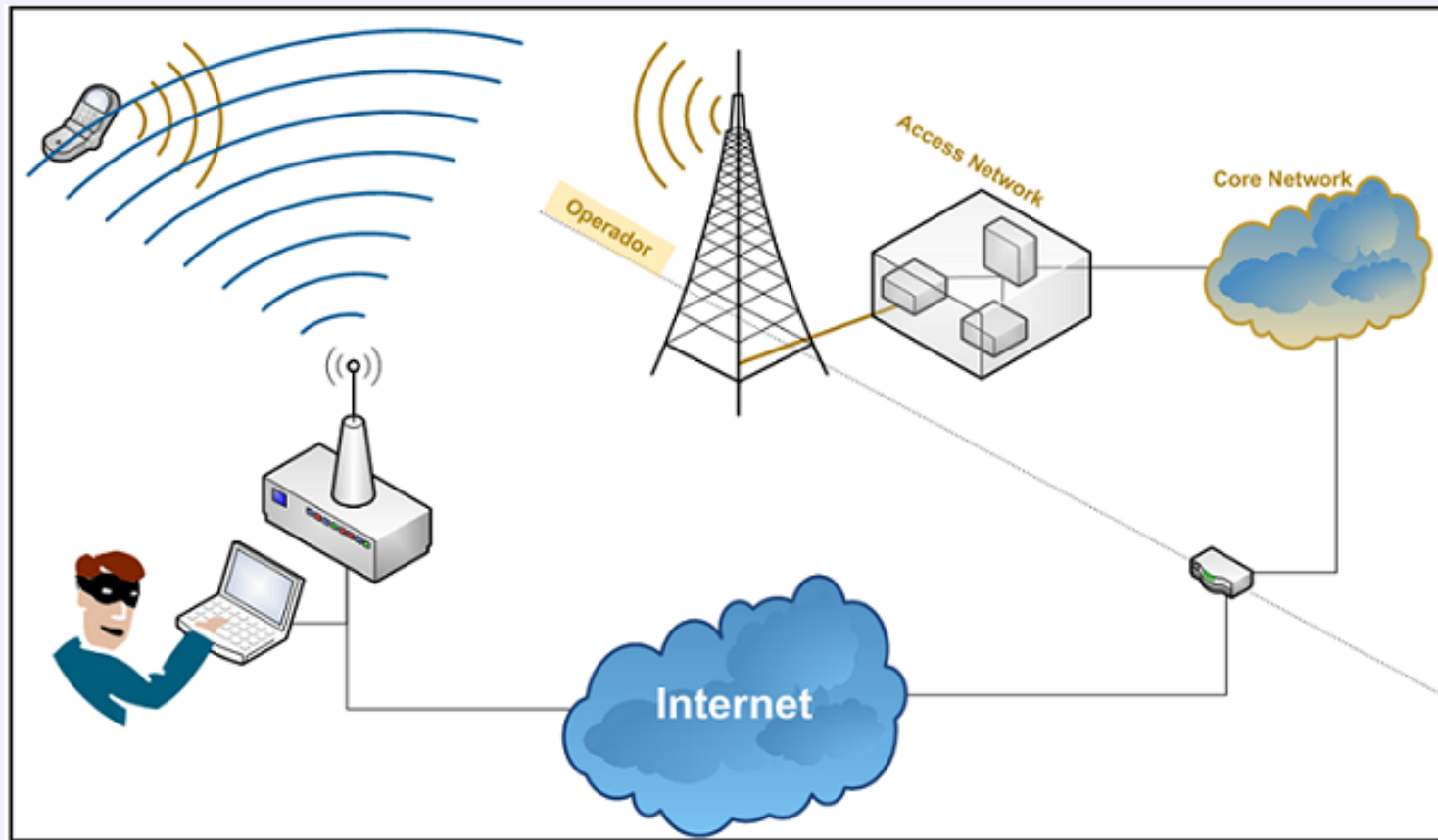
- Jaula de Faraday para realizar pruebas...



OWASP

The Open Web Application Security Project

Rogue BTS en la red Real del operador





Ataques complementarios

- Denegación de servicio selectiva y persistente
- Redirección de llamadas de la víctima
- Llamada a víctima con suplantación de víctima
- Grabación de cualquier llamada de la víctima
- Captura de cualquier SMS enviado por la víctima



OWASP

The Open Web Application Security Project



Sobre la Seguridad en GSM..

- ~~Autenticación del usuario~~
- ~~Confidencialidad en las comunicaciones de señalización y de usuario~~
- ~~Confidencialidad de datos de usuario~~
- ~~Autenticación de la red~~



OWASP

The Open Web Application Security Project

SEGURIDAD EN GPRS

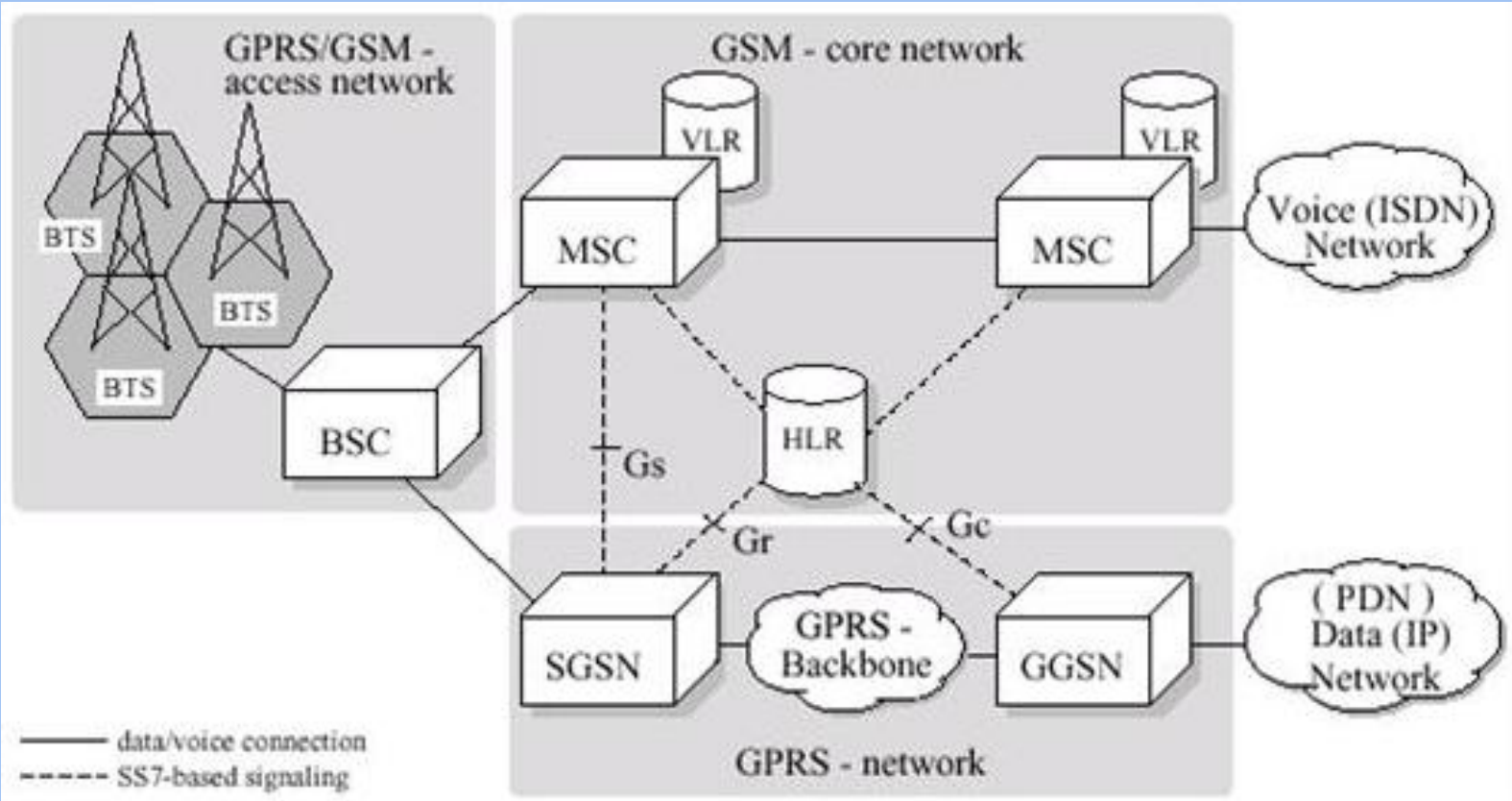




OWASP

The Open Web Application Security Project

Arquitectura GPRS





OWASP

The Open Web Application Security Project

Comparación con GSM

Autenticación de la red

- Tampoco existe

Confidencialidad de la identidad del usuario

- Idéntico problema a GSM (uso de identificadores temporales -PTMSI- y obligatoriedad de contestar a la red ante la solicitud de IMSI)

Confidencialidad de la información de datos y señalización

- Comprometida por:
 - Obligatoriedad de soportar GEA/0
 - Criptoanálisis del algoritmo GEA/1

Autenticación del usuario

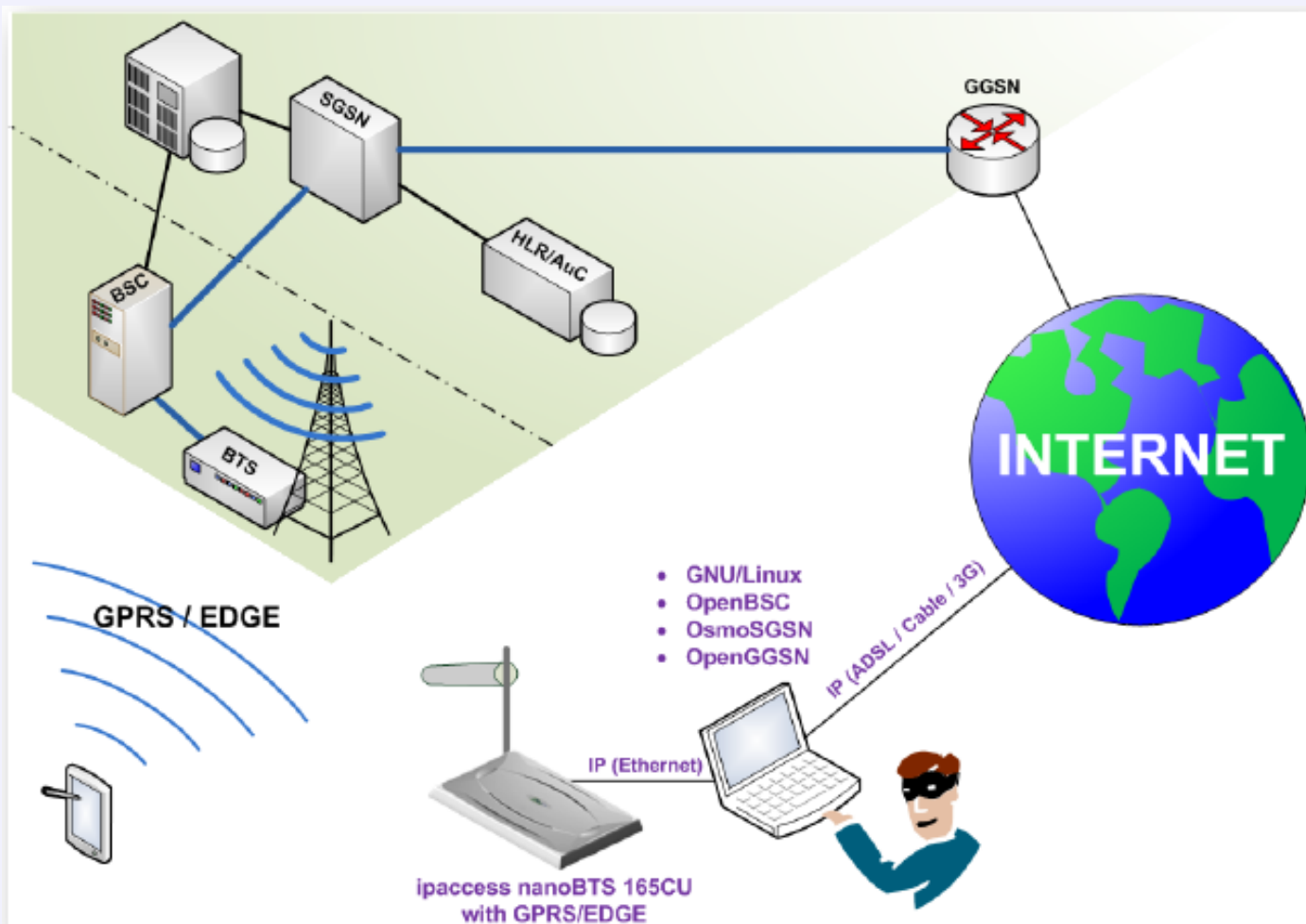
- Comprometida por la posibilidad de obtener GPRS Kc



OWASP

The Open Web Application Security Project

Ejecución del ataque





OWASP

The Open Web Application Security Project

Conclusiones y Recomendaciones



Completamente vulnerable....



OWASP

The Open Web Application Security Project



OWASP

Mobile Security Project

The OWASP Mobile Security Project is a centralized resource intended to give developers and security teams the resources they need to build and maintain secure mobile applications. Through the project, our goal is to classify mobile security risks and provide developmental controls to reduce their impact or likelihood of exploitation.

Our primary focus is at the application layer. While we take into consideration the underlying mobile platform and carrier inherent risks when threat modeling and building controls, we are targeting the areas that the average developer can make a difference. Additionally, we focus not only on the mobile applications deployed to end user devices, but also on the broader server-side infrastructure which the mobile apps communicate with. We focus heavily on the integration between the mobile application, remote authentication services, and cloud platform-specific features.

- https://www.owasp.org/index.php/OWASP_Mobile_Security_Project



OWASP

The Open Web Application Security Project

- Mobile Top 10 2016-Top 10

M1 - Improper Platform Usage

M2 - Insecure Data Storage

M3 - Insecure Communication

M4 - Insecure Authentication

M5 - Insufficient Cryptography

M6 - Insecure Authorization

M7 - Client Code Quality

M8 - Code Tampering

M9 - Reverse Engineering

M10 - Extraneous Functionality



OWASP

The Open Web Application Security Project

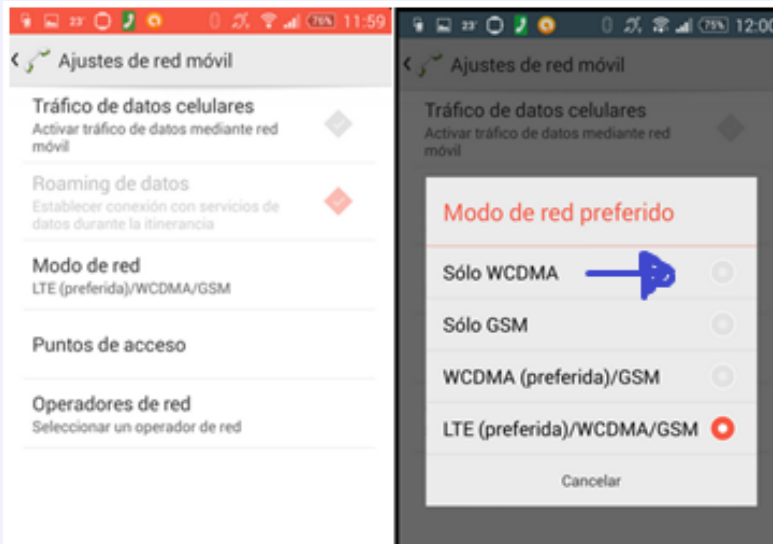
Conclusiones y Recomendaciones



Completamente vulnerable....

Recomendaciones

- Configuración del terminal para que utilice 3G o superior





OWASP

The Open Web Application Security Project

- Desarrollo de software para dispositivos móviles de alerta del modo de cifrado en los terminales
- Soluciones basadas en la detección de estaciones base falsas
 - Implementación de HW y SW que detecte la presencia de estaciones Base falsas
- Soluciones basadas en cifrado a través de los canales CSD de GSM
- Soluciones basadas en VoIP cifrado
- Protección de la comunicación en niveles superiores



OWASP
The Open Web Applicati





OWASP

The Open Web Application Security Project

Gracias!!!



mauricanseco@yahoo.com



@Madklux



es.linkedin.com/in/mauriciocansecotorres