

Universidad Argentina John F. Kennedy

Licenciatura en Sistemas

**Pago por medio del Celular:**Fácil, seguro, en cualquier celular y lugar

Juan Ignacio Carson

TUTOR

Junio 2014

Abstract

En la actualidad el teléfono celular es usado como plataforma para nuevas formas de pago. Pero no se puede acceder a ellas con modelos antiguos o cuando no se tiene acceso a internet.

Este trabajo propone transformar cualquier celular en un medio de pago viable y seguro. Para ello se utilizara el servicio SMS de la actual red GSM, disponible en cualquier lugar y para cualquier modelo, como canal de comunicación entre el servidor de la compañía que ofrece el servicio de pago y los clientes y comerciantes que lo utilizaran.

Para poder realizar transacciones de forma segura se protegerá el sistema de las vulnerabilidades propias de las telecomunicaciones en la red GSM, de los problemas relacionados con la seguridad física del dispositivo, como también de los generados por el factor humano.

De esta manera el pago a través de SMS se transformara en un medio seguro, disponible en cualquier lugar y fácil de usar como lo son hoy las tarjetas de crédito.

Contenido

[Introducción 2](#_Toc405622083)

[Justificación 3](#_Toc405622084)

[Problemática 4](#_Toc405622085)

[Objetivo General 5](#_Toc405622086)

[Objetivos Específicos 5](#_Toc405622087)

[Alcances y Limites 6](#_Toc405622088)

[Hipótesis 7](#_Toc405622089)

[Metodología 8](#_Toc405622090)

[Mapa conceptual 9](#_Toc405622091)

[Estado del Arte 10](#_Toc405622092)

[Marco teórico 11](#_Toc405622093)

[Seguridad de GSM 11](#_Toc405622094)

[Intercepcion de SMS con Software Defined Radio 11](#_Toc405622095)

[Des encriptar llamadas GSM 12](#_Toc405622096)

[Hacking en redes GSM con RTL-SDR 14](#_Toc405622097)

[Desarrollo 18](#_Toc405622098)

[Conclusiones 19](#_Toc405622099)

# Introducción

Los más modernos teléfonos celulares proponen ser utilizados para realizar pagos entre personas y empresas, para ello disponen de tecnología NFC (Near field communication) e Internet. Pero los teléfonos celulares más antiguos no cuentan con tecnologías modernas como NFC y tampoco la cobertura de internet no alcanza todos los puntos del país.

La razón de este trabajo es que cualquiera pueda utilizar el teléfono celular como medio de pago. Para lograrlo se propone que una compañía operadora de telefonía celular brinde el servicio de pago por celular y utilice el servicio SMS de la red GSM, del cual todos los celulares disponen, como medio de comunicación entre los celulares que utilizan el servicio y el servidor que brinda el servicio de la operadora de telefonía celular.

El producto resultante permite a un comerciante enviar por SMS el importe a cobrar a la operadora, la cual envía un PIN al comerciante que se encuentra asociado al importe solicitado y al comerciante. Este PIN es mostrado al cliente que lo envía por SMS a la operadora. Esta última al recibir el PIN asociado a un importe y comerciante transfiere el importe de la cuenta del cliente a la cuenta del comerciante.

Debe ser fácil de usar tanto para el cliente como el comerciante y también debe subsanar problemas de seguridad de los celulares, del medio de comunicación utilizado y los generados por las personas que utilizaran el servicio.

# Justificación

La tecnología avanza cada vez más rápido y las novedades son cada vez más caras e inaccesibles para muchas personas y países. Razón por la cual hay personas que no tienen los últimos Smartphones con tecnologías más nuevas y también hay países que no tienen cobertura 3g en todo su territorio.

La novedad que resulta el teléfono móvil como medio de pago no tiene por qué ser solo accesible para las personas y países que tienen más recursos. Y esa es la razón por la cual este proyecto se basa en una tecnología utilizada tanto por los que tienen pocos recursos y los que tienen muchos.

# Problemática

Hoy el teléfono móvil se propone como medio de pago peor las distintas implementaciones no tiene total cobertura y el servicio que brindan solo puede ser utilizado por una parte de los usuarios de telefonía móvil. Este es el problema que se propone solucionar el proyecto transformando cualquier celular en un medio de pago que podrá ser usado en cualquier lugar con cobertura GSM.

# Objetivo General

Demostrar que cualquier celular puede ser utilizado como medio de pago usando como canal de comunicación el servicio SMS.

# Objetivos Específicos

Simplificar la operatoria a realizar sea para que sea fácil para cualquier individuo.

Hacer que este servicio de pago sea al menos tan seguro como lo es usar una tarjeta de crédito.

# Alcances y Limites

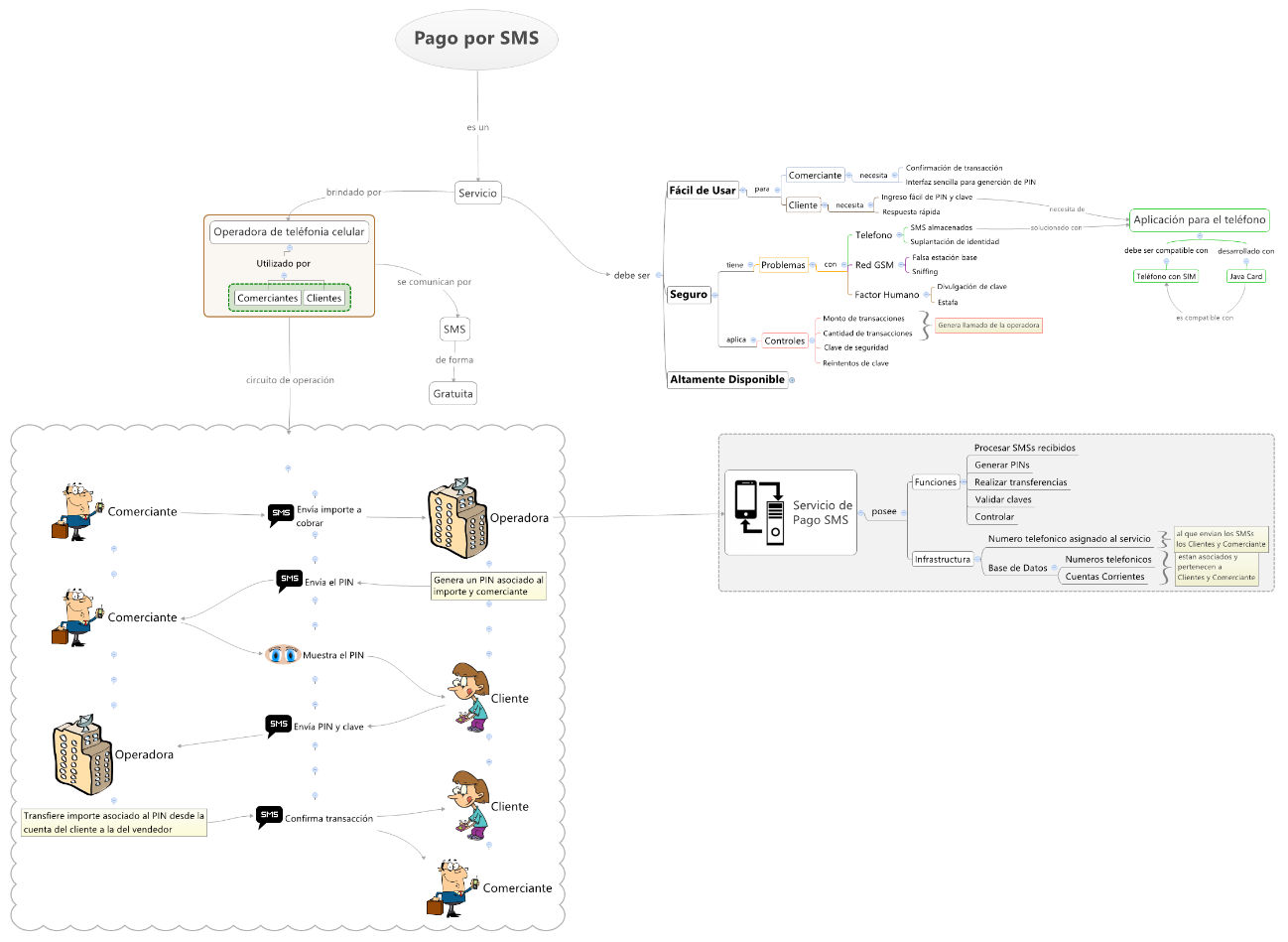
# Hipótesis

Se pueden utilizar todos los celulares con capacidad de enviar SMS como medios de pago.

El SMS como medio de pago puede ser al menos tan seguro como una tarjeta de crédito.

# Metodología

# Mapa conceptual



# Estado del Arte

Varias empresas ofrecen distintos servicios de diversos tipos a través del SMS. Los más similares al producto que se quiere lograr en este proyecto son los de transferencia de saldo que brindan varias compañías de telefonía celular, el cual permite a los abonados transferir saldo telefónico y de SMSs a otros usuarios. Otro servicio que se asemeja es el que brindan los bancos, el cual permite realizar consultas de saldo y transferencias bancarias a cuentas previamente autorizadas.

# Marco teórico

## Seguridad de GSM

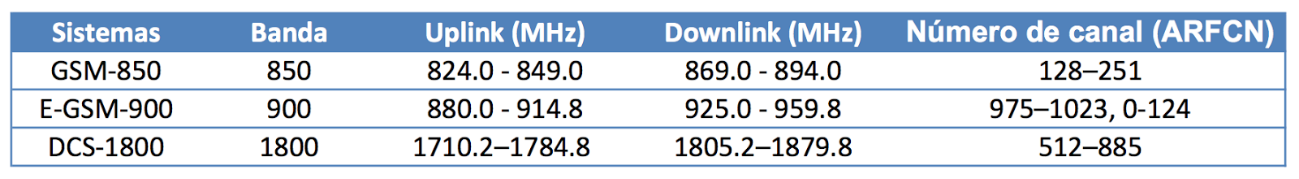
Uno de los aspectos a analizar en el proyecto es la seguridad que brinda GSM para ello vamos a resumir los problemas conocidos.

### Hacking en redes GSM con RTL-SDR

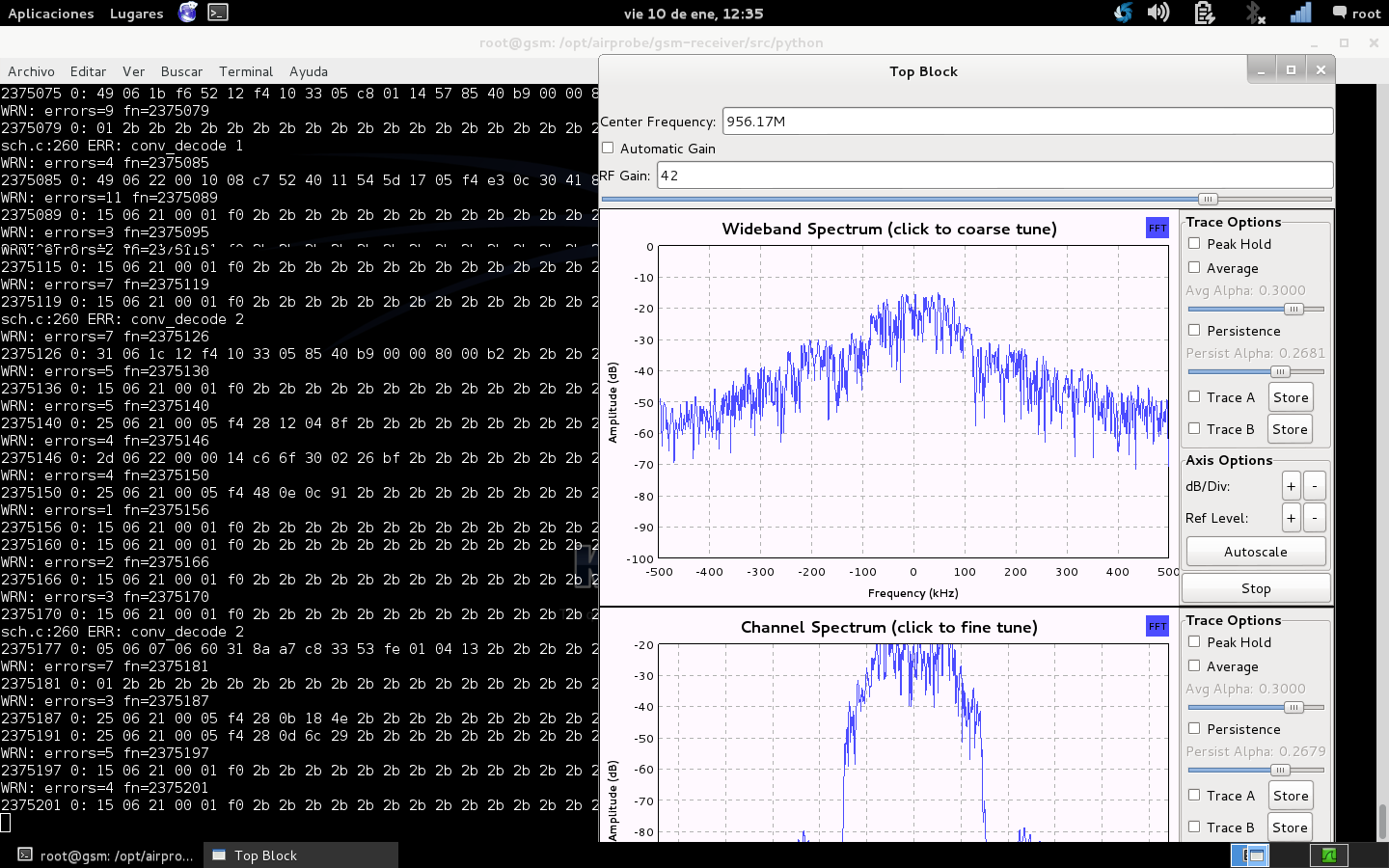
El escenario actual sobre ataques a la red GSM ha ido evolucionando y ya no hace falta modificar teléfonos con chipset Calypso ni un hardware complejo como los USRP (+/- 900 €). La culpa de esto la tiene el chipset de RealTek RTL2832U. Este chipset está presente en varios modelos de sintonizadores TDT con un precio que oscila entre 20 y 30 Euros y que se pueden adquirir en Internet.

Además, hace unos años, los señores del Software Defined Radio (SDR) se fijaron en ellos porque podían utilizar el sintonizador en un rango más amplio que su utilidad original de sintonizar la TDT - para ver todos los usos posibles acudir a RTL-SDR, donde se pueden ver usos como la detección de meteoritos, el seguimiento de aviones, comunicaciones TETRA, etcétera, etcétera.

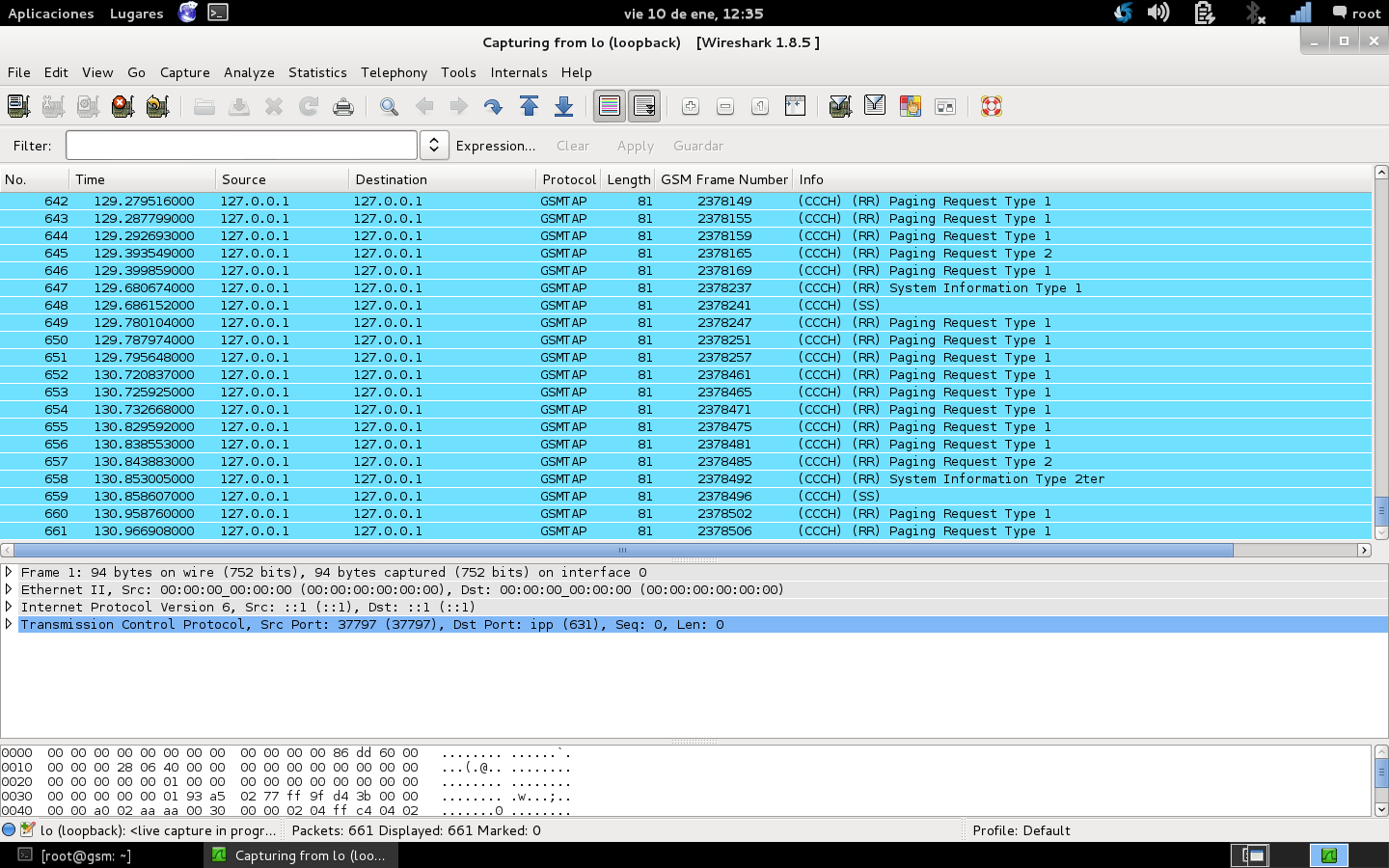
Dependiendo de los fabricantes el rango de frecuencias que puede capturar cada dispositivo oscila, pero podemos decir que el rango de frecuencias (Elonics E4000) es de 52 a 2200 MHz y la gran suerte (o no) es que dentro de ese rango, tenemos las bandas utilizadas en la telefonía móvil:



Con todo esto, el proyecto OpenSource OsmoSDR se encargó de escribir el software necesario para manejar estos dispositivos y poder capturar la señalización que viaja por el "aire" a un fichero binario, pudiendo ajustar la frecuencia, el ancho de banda, ganancia, etcétera.



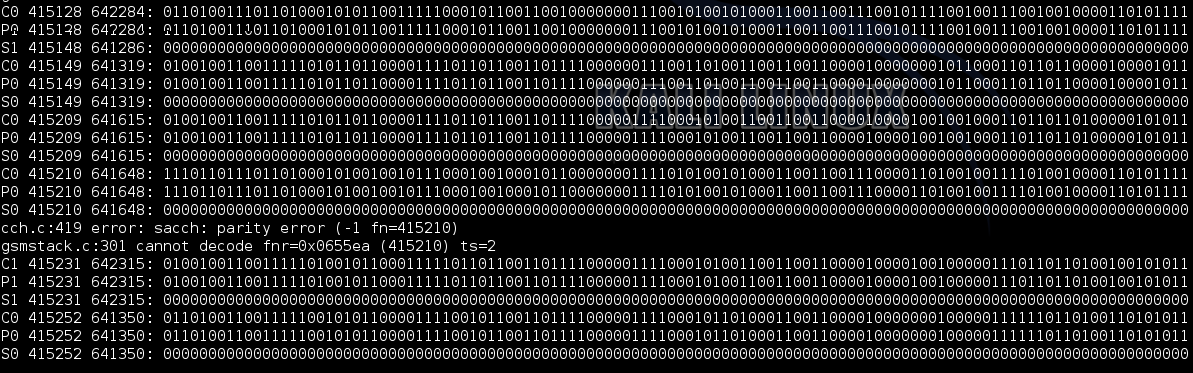
Utilizando el software del GNU Radio Companion se puede adaptar de manera muy sencilla el formato de este fichero binario al formato que utiliza el programa airprobe, encargado de decodificar la señalización capturada con varios tipos de dispositivos (RTL-SDR, USRP, etcétera)



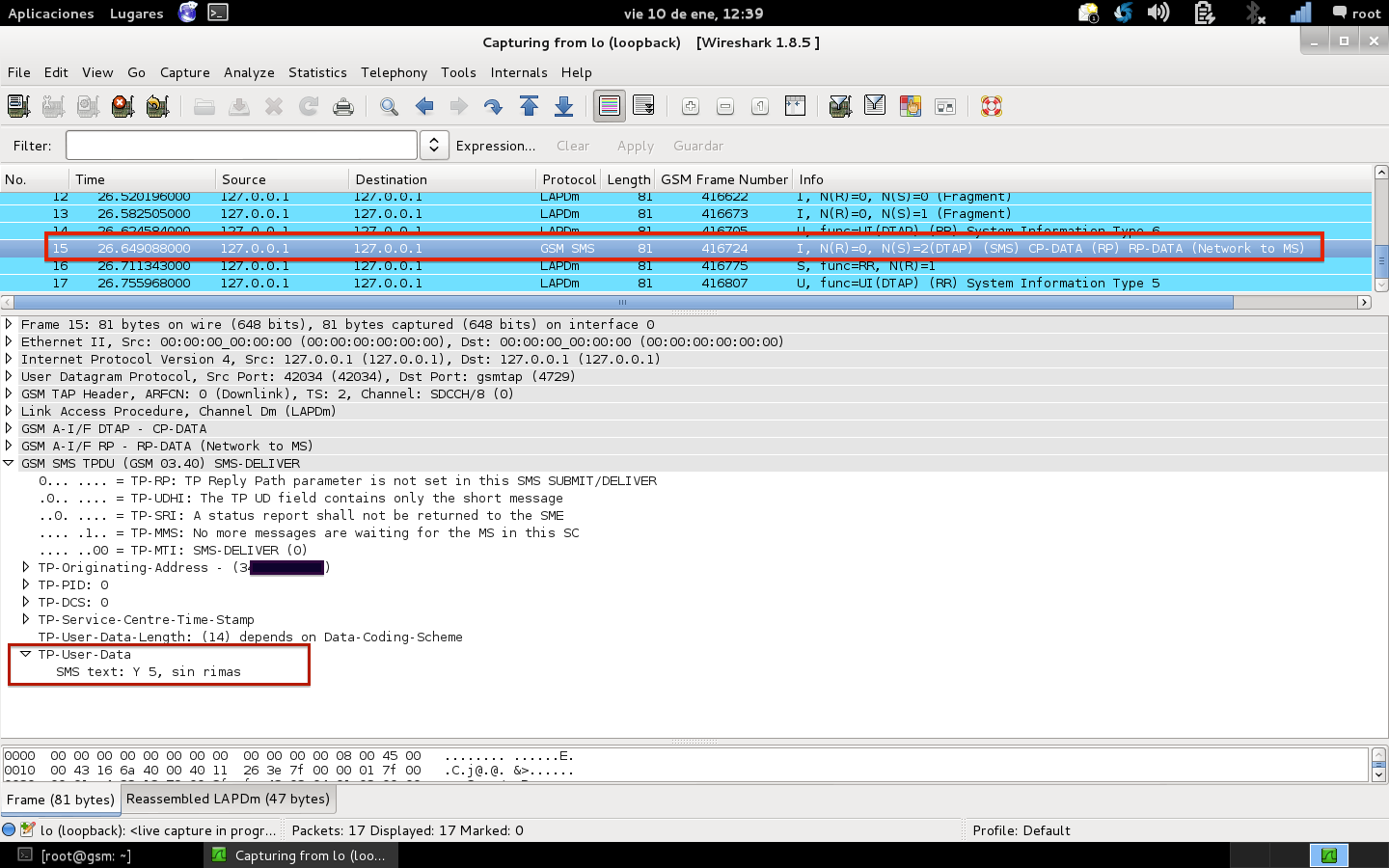
Esto ya permitiría a cualquiera capturar el tráfico que está pasando por una determinada frecuencia y verlo en su analizador de tráfico preferido. En este caso podemos ver la señal en Wireshark, pero por supuesto todo irá cifrado con A5/1. El último paso es crackear la información que viaja por el aire cifrada.



Se supone que este paso debería de resultar "imposible" para cualquier hijo de vecino, pero la realidad es muy triste y no es así. Cualquiera puede descifrar esta información, puesto que el algoritmo utilizado para cifrar las comunicaciones (A5/1) es demasiado viejo (1988) y ya demostró Karsten Nohl cómo romperlo utilizando sus Rainbow Tables, aunque en 1997 ya se había probado teóricamente cómo romperlo.



Es decir, con 20€ y un equipo con una distribución de Kali Linux, cualquier persona con muy pocos conocimientos puede realizar capturas de todo el tráfico de una celda de la red GSM para más tarde, en su casa, descifrar el tráfico en busca de llamadas y mensajes cortos, ¿A que pone los pelos de punta? Pensad en ello la próxima vez que recibáis un SMS con una información sensible.



  
Tarjeta RTL-SDL por USB necesaria

### Intercepcion de SMS con Software Defined Radio

The possible intercepting scenario looks as follows. We send a test SMS message to our phone and use a special device to intercept the radio signal from the base station. We then decode and decrypt captured SMS message.

In our work we describe the concepts and implementation of passively intercepting SMS text messages over GSM’s air interface by means of the software defined radio called USRP (Universal Software Radio Peripheral).

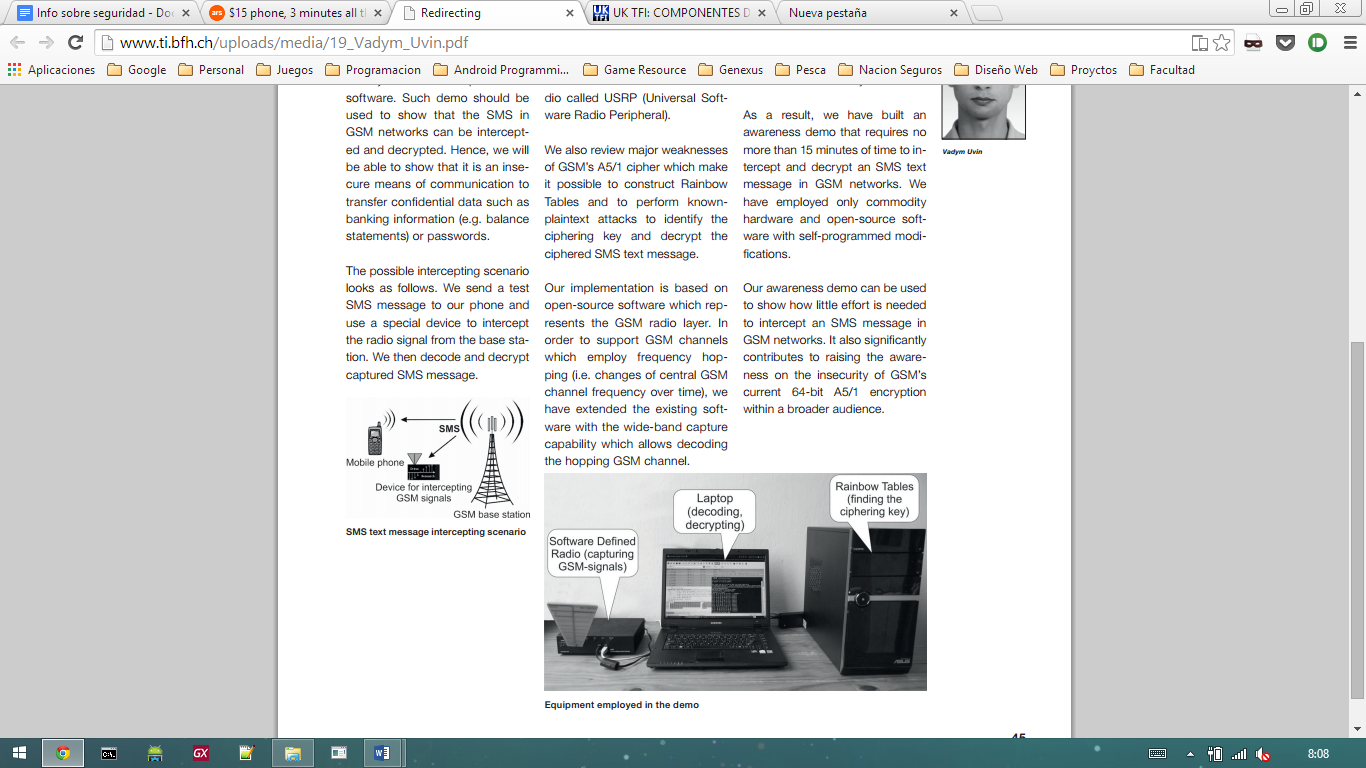
We also review major weaknesses of GSM’s A5/1 cipher which make it possible to construct Rainbow Tables and to perform knownplaintext attacks to identify the ciphering key and decrypt the ciphered SMS text message.

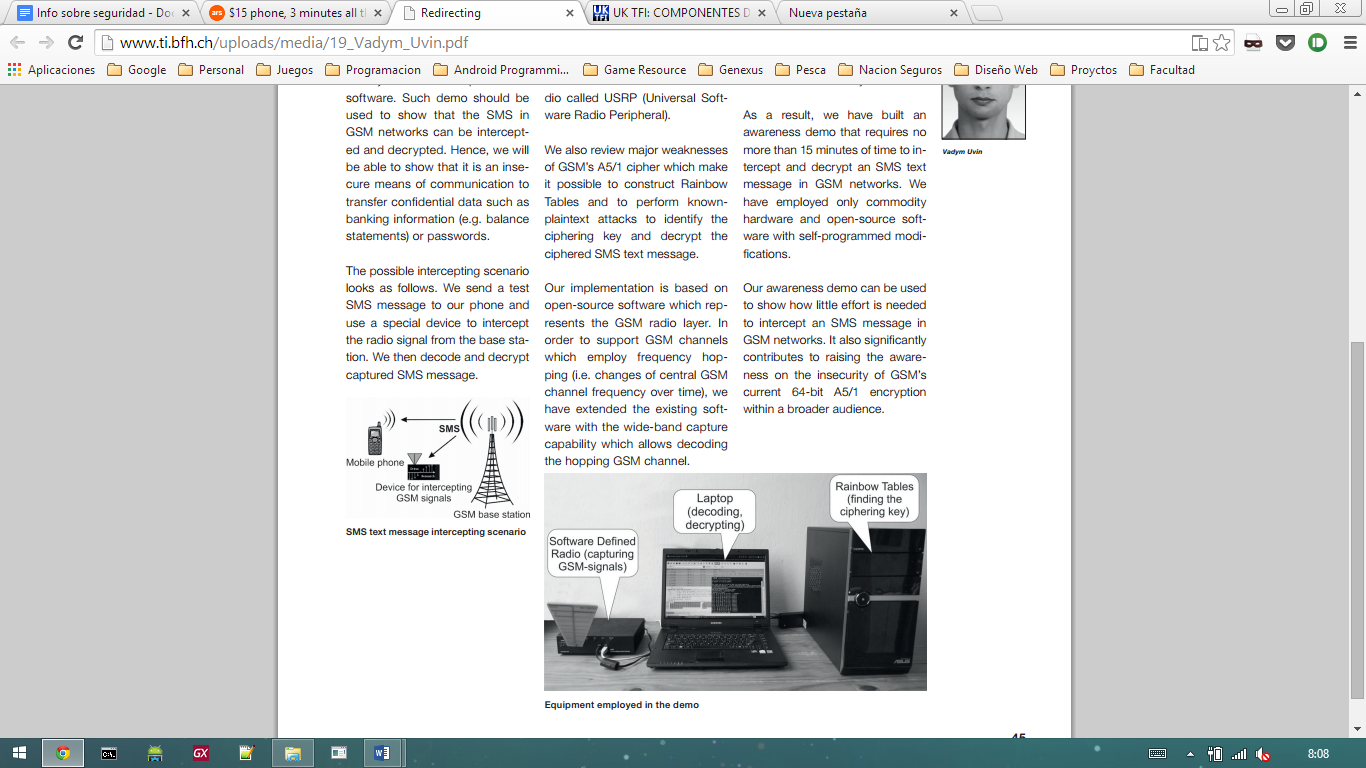
Our implementation is based on open-source software which represents the GSM radio layer. In order to support GSM channels which employ frequency hopping (i.e. changes of central GSM channel frequency over time), we have extended the existing software with the wide-band capture capability which allows decoding the hopping GSM channel.

Our demo is based on self-programmed Python scripts which make it easier to perform attacks on the GSM A5/1 cipher in order to find the session key.

As a result, we have built an awareness demo that requires no more than 15 minutes of time to intercept and decrypt an SMS text message in GSM networks. We have employed only commodity hardware and open-source software with self-programmed modifications.

Our awareness demo can be used to show how little effort is needed to intercept an SMS message in GSM networks. It also significantly contributes to raising the awareness on the insecurity of GSM’s current 64-bit A5/1 encryption within a broader audience.





### Des encriptar llamadas GSM

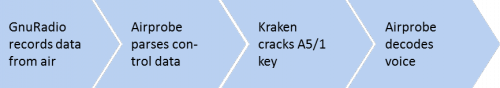
**Motivation**. GSM telephony is the world’s most popular communication technology spanning most countries and connecting over four billion devices. The security standards for voice and text messaging date back to 1990 and have never been overhauled. Our GSM Security Project creates tools to test and document vulnerabilities in GSM networks around the world so to ignite the discussion over whether GSM calls can and should be secured. The project is summarized in this BlackHat 2010 presentation.

**Recording calls**. GSM data can be recorded off the air using, for example, a programmable radio such as the USRP. GnuRadio provides the tools to record channels while Airprobe’s gsm-receiver decodes the control traffic and in scenarios where no encryption is used or where the encryption key is known also decodes voice traffic.

**Cracking A5/1**. When GSM uses A5/1 encryption, the secret key can be extracted from recorded traffic. Given two encrypted known plaintext messages, the Kraken utility that runs on a PC finds the secret key with around 90% probability within seconds in a set of rainbow tables. Our current table set took 2 months to compute and contains 40 tables for a total of 2TB. Further details on cracking A5/1 using rainbow tables are provided in this white paper: Attacking Phone Privacy.

**Defenses**. Short term protocol patches already exists that make cracking much harder by not disclosing known plaintext unnecessarily (3GPP TS44.006, Section 5.2). These patched should be deployed with high priority. In the long term, GSM (2G) will not provide sufficient security and stronger alternatives such as UMTS (3G) and LTE (4G) should be preferred.

**Tools**. The following tools are used to analyze voice calls



* GnuRadio is included in recent Linux distributions  
  Recording data requires a programmable radio receiver such as the USRP
* Airprobe is available through:   
  git clone git://git.gnumonks.org/airprobe.git  
  Please follow this tutorial to decode GSM traffic with Airprobe
* Kraken is available through:   
  git clone git://git.srlabs.de/kraken.git  
  Background on Kraken’s rainbow tables are provided on the project web page  
  Kraken uses rainbow tables that are available through Bittorrent.

Please use these tools carefully and never intentionally record other people’s conversations. We do encourage you to use them to test the security of your cell phone service and discuss your results on the project mailing list.

# Desarrollo

# Conclusiones