A fragilidade da implementação de redes GSM no Brasil

Igor Marcel e Wilberto Filho

GSM

Definição, surgimento e características

GSM

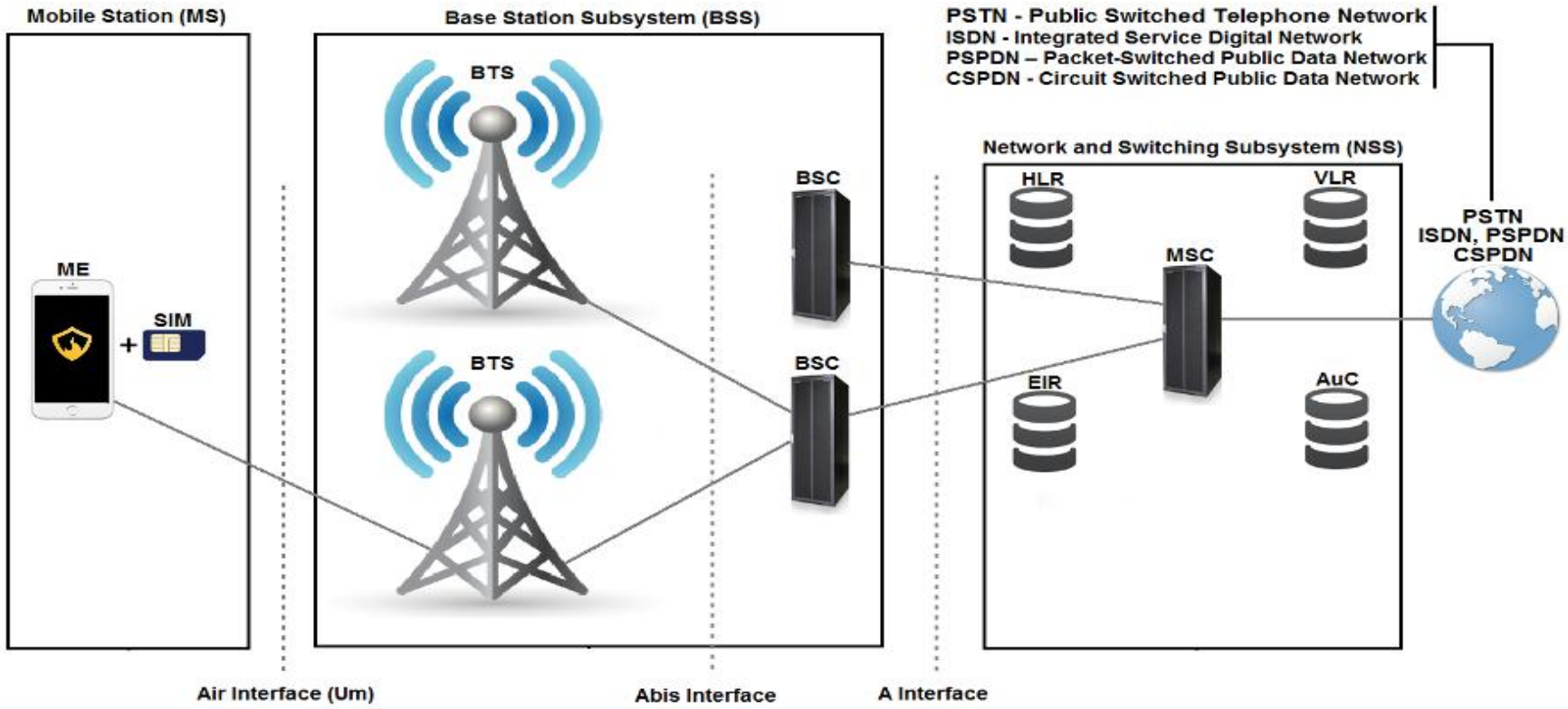
Global System for Mobile Communications

Groupe Spécial Mobile

GSM

GSM

Arquitetura do sistema GSM convencional



ME - Mobile Equipment
SIM - Subscriber Identity Module

BTS - Base Transceiver Station
BSC - Base Station Controller

HLR - Home Location Register
VLR - Visitor Location Register
MSC - Mobile Switching Center
EIR - Equipment Identity Register
AuC - Authentication Center

GSM – Bandas de frequência

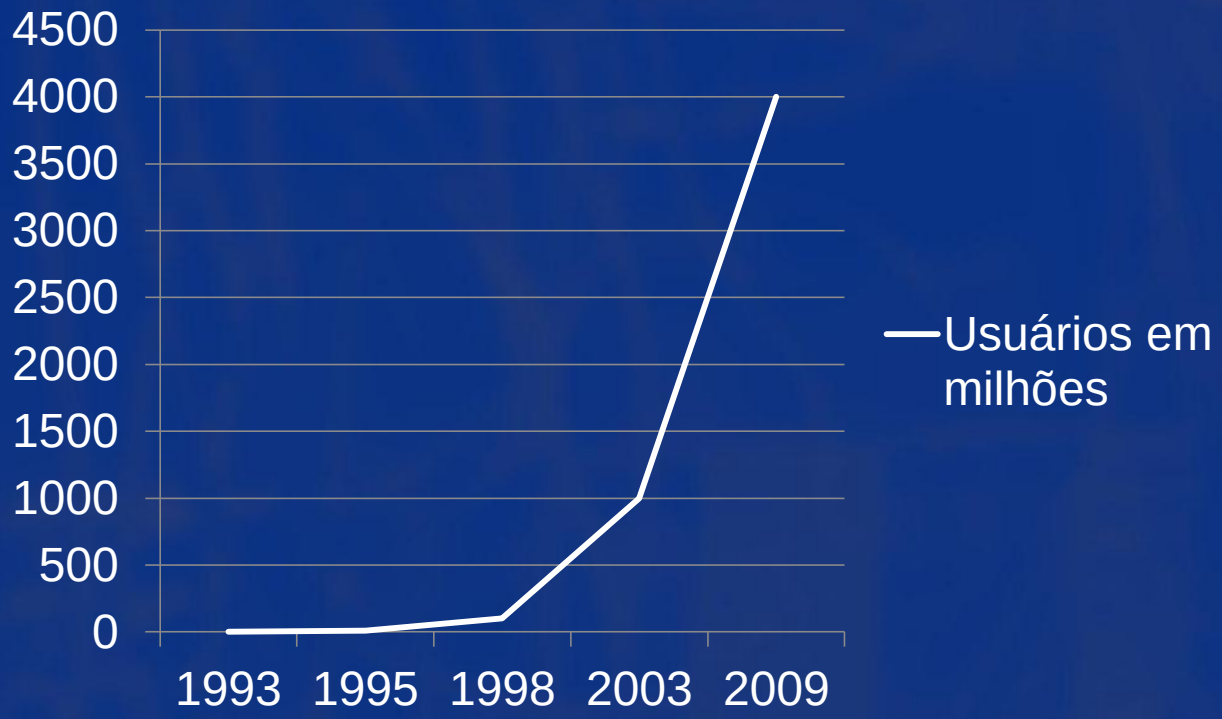
GSM – Bandas de frequência

O padrão 3GPP TS 45.005 define 14 classes de bandas de frequência GSM, porém, falaremos apenas das quatro bandas globalmente padronizadas para fins comerciais.

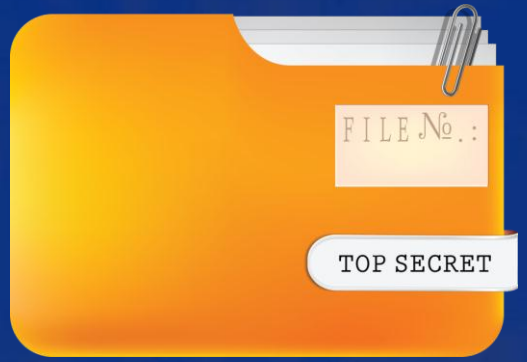
GSM – Bandas de frequência

SISTEMA	BANDA	UPLINK (MHz)	DOWNLINK (MHz)	REGIÃO
GSM 850	850	824 - 849	869 - 894	América do Norte, Caribe e América Latina
E-GSM 900	900	880 - 915	925 - 960	Europa, Oriente Médio, África e Ásia
DCS 1800	1800	1,710 - 1 ,785	1,805 - 1,880	Europa, Oriente Médio, África e Ásia
PCS 1900	1900	1,850 – 1,909	1,930 – 1,989	América do Norte, Caribe e América Latina

GSM – Crescimento



GSM - Uso



GSM

Redes GSM no Brasil

Se funcionou está bom!

Redes GSM no Brasil

Reutilização de equipamento antigo

Redes GSM no Brasil

Não segue padrão preestabelecido

Redes GSM no Brasil

Desabilitação de funcionalidades de segurança

Nosso laboratório

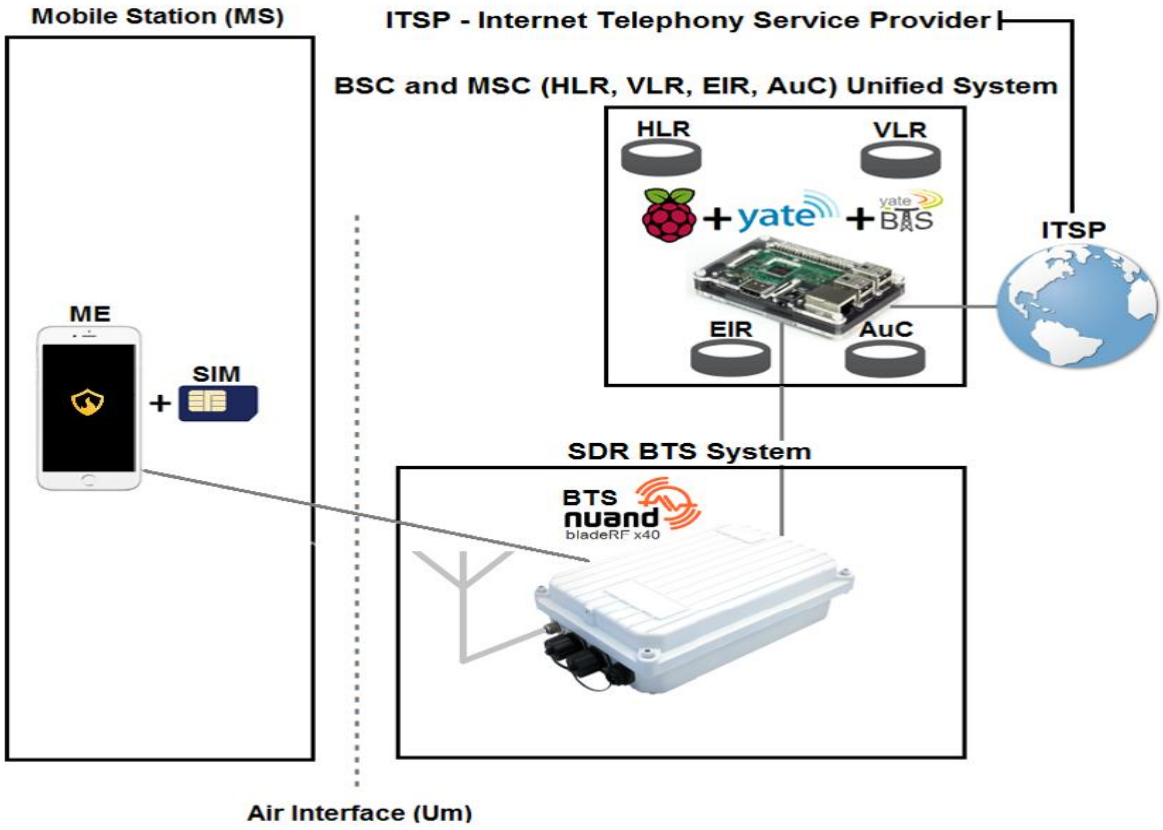
Hardware, software e arquitetura

BTS portátil = BlazeBTS

HARDWARE	PREÇO
Nuand bladeRF x40 (USB 3.0 Superspeed Software Defined Radio)	$420,00
Duas antenas Quadriband para celular com conectores SMA	$15,09
Kit Raspberry Pi 3 (modelo B)	$69,00
Carregador portátil Anker Astro E7 - 26800mAh (opcional)	$54,00

SOFTWARE	PREÇO
RASPBIAN Jessie Lite (March 2016, Release date: 2016-03-18, Kernel version 4.1)	Gratuito
Yate (Yet Another Telephony Engine)	Gratuito (versão pública)
YateBTS	Gratuito (versão pública)

Arquitetura do sistema GSM unificado



ME - Mobile Equipment
SIM - Subscriber Identity Module
SDR - Software Defined Radio
BTS - Base Transceiver Station
BSC - Base Station Controller

HLR - Home Location Register
VLR - Visitor Location Register
MSC - Mobile Switching Center
EIR - Equipment Identity Register
AuC - Authentication Center

O bom e o mau uso de nossa BTS

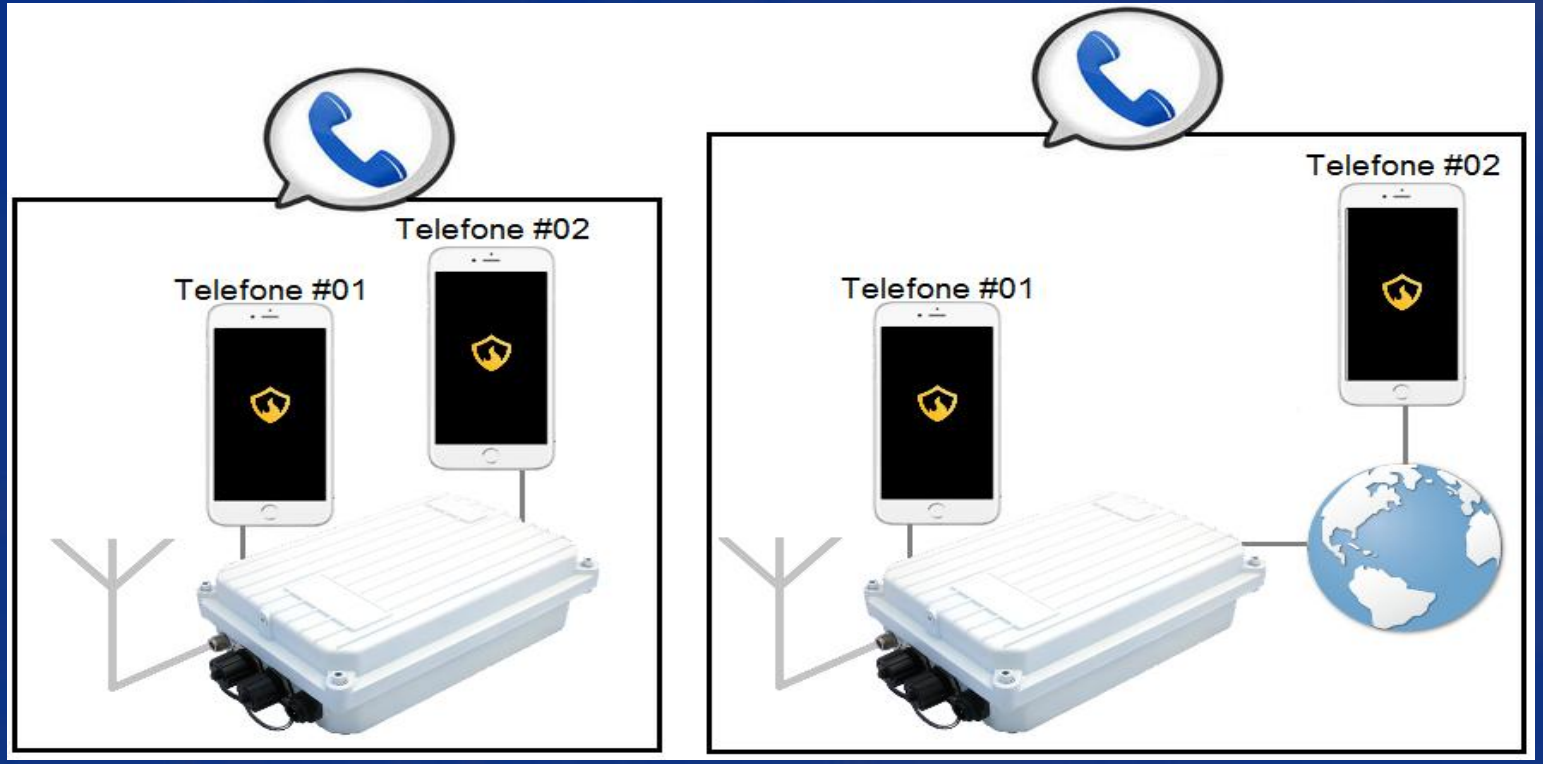
Ataques que podem ser executados

- Interceptar e ou redirecionar chamadas de voz
- Interceptar e ou redirecionar mensagens SMS
- Interceptar e ou redirecionar o tráfego de dados GPRS
- Spoofar números telefônicos
- Spoofar BTSs legítimas de operadoras locais (Oi, TIM, Vivo, Claro...)
- Agir como um IMSI-Catcher (StingRay, Triggerfish, Piranha, Kingfish...)
- Desconectar e ou negar a conexão de estações móveis de uma determinada área

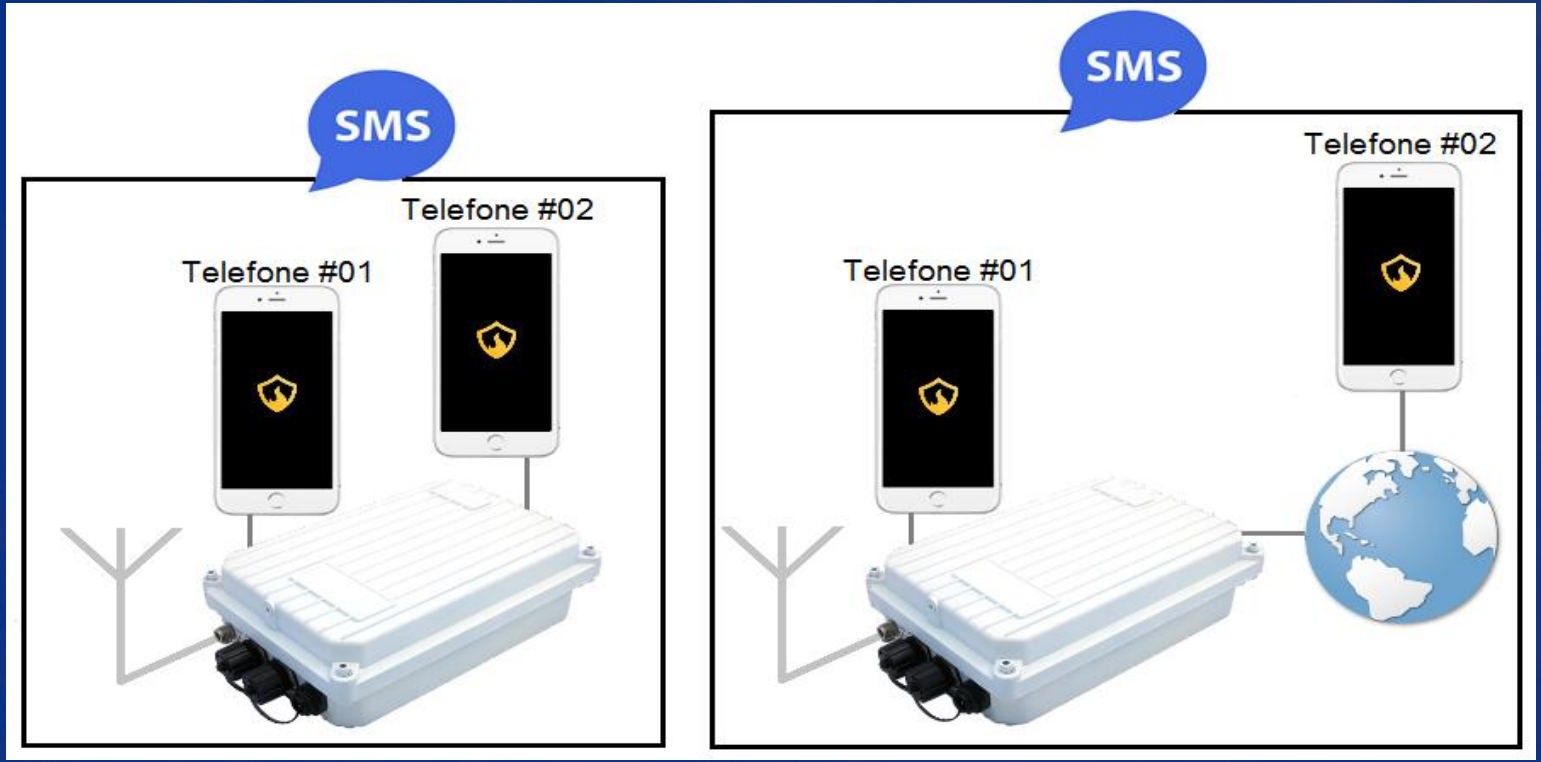
Ataques

Aqui é onde a brincadeira começa,
bem-vindos ao Mind The Sec 2016!

Interceptação de chamadas de voz



Interceptação de SMS

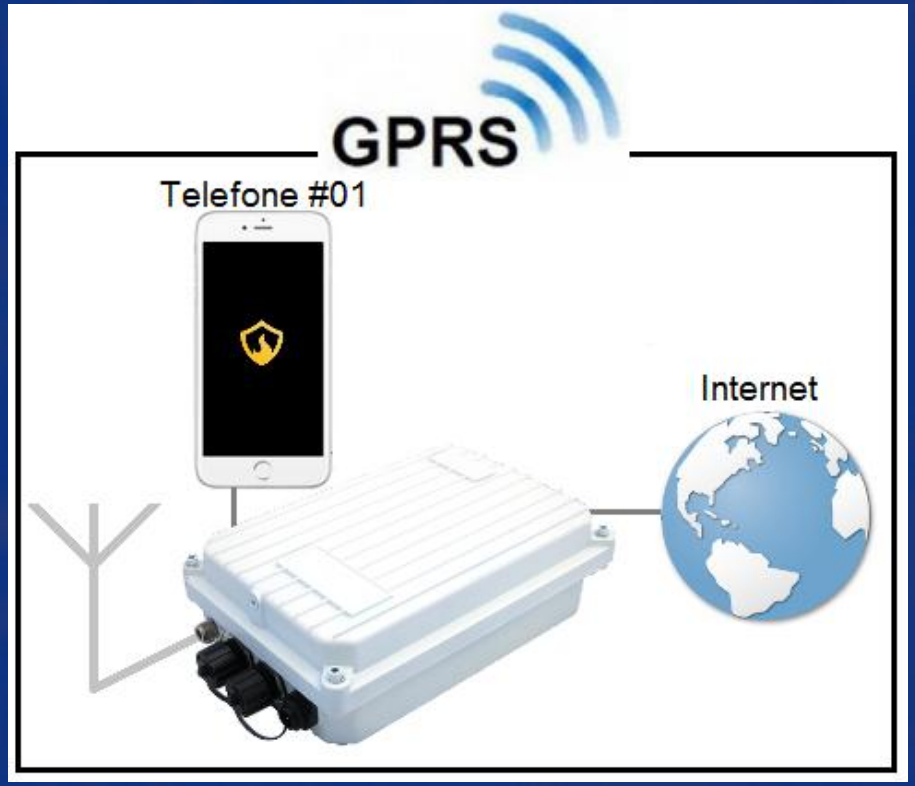


Spoofing de número telefônico

FLIPSIDE - http://www.flipside.com.br/

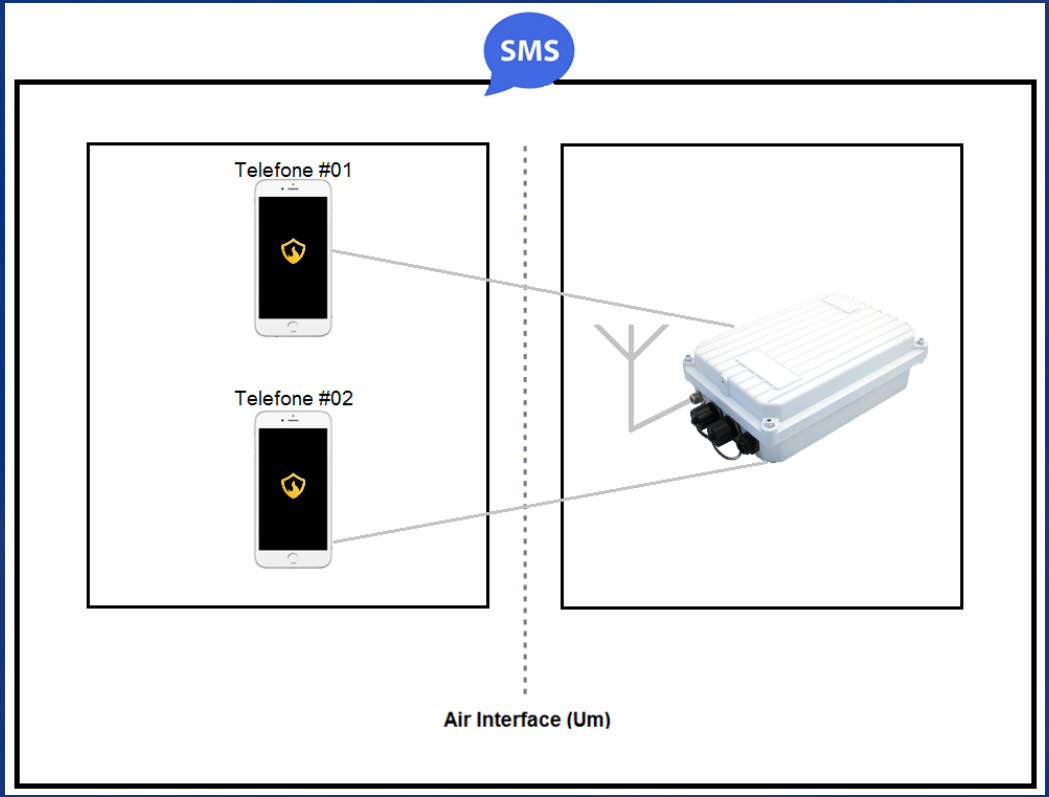
TELEFONE: +55 (11) 3256-5724

Interceptação de dados (GPRS)

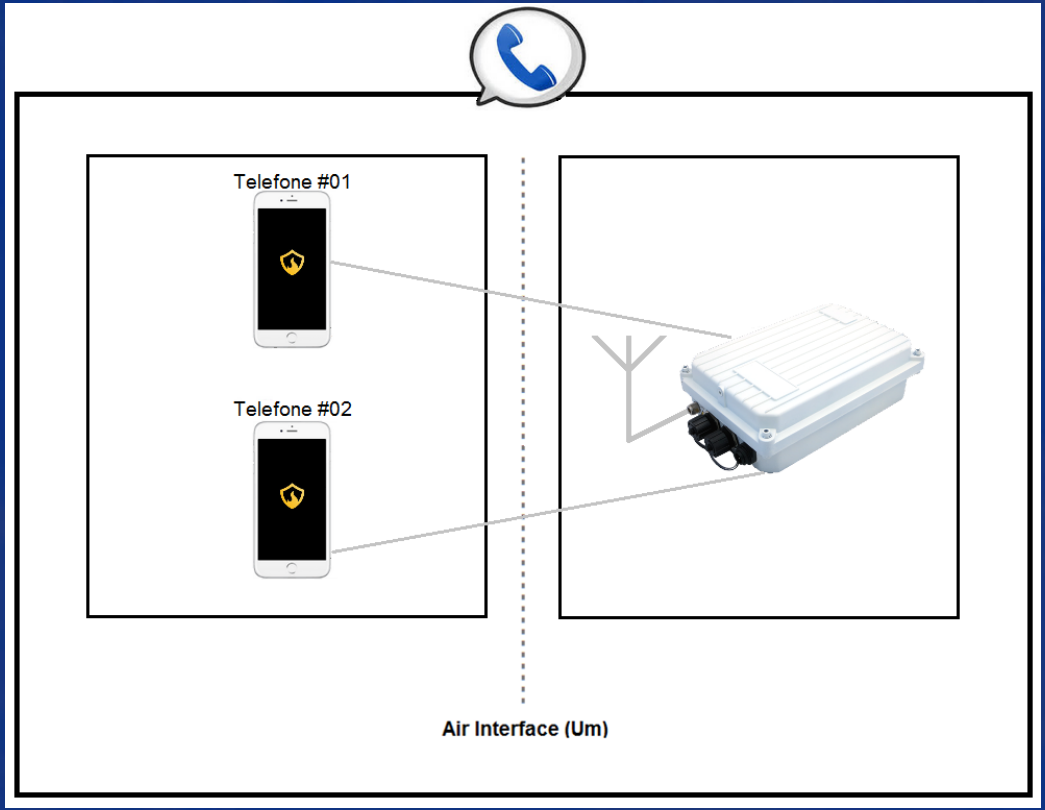


RTL-SDR

Interceptação de SMS (RTL-SDR)



Interceptação de voz (RTL-SDR)



Próximas pesquisas e ataques

Ainda há bastante assunto para estudar!

Ainda há bastante espaço para pesquisas futuras relacionadas à tecnologia GSM.

O baixo custo da implementação do ambiente descrito possibilita que profissionais de segurança e hackers pesquisem por vetores de ataques mais sofisticados.

Alguns exemplos

- Ataques do tipo OTA (over-the-air)
- Ataques do tipo Evilgrade
- Ataques direcionados ao baseband das estações móveis
- Ataques direcionados a protocolos específicos
- Fuzzing de SMS

Referências

Intercepting GSM Traffic
(David Hulton and Steve)
https://www.blackhat.com/presentations/bh-dc-08/Steve-DHulton/Whitepaper/bh-dc-08-steve-dhulton-WP.pdf

GSM: SRSLY?
(Karsten Nohl and Chris Paget)
https://events.ccc.de/congress/2009/Fahrplan/attachments/1519_26C3.Karsten.Nohl.GSM.pdf

IMSI-Catcher and Man-in-the-Middle Attacks
(Julian Dammann)
https://cosec.bit.uni-bonn.de/fileadmin/user_upload/teaching/10ws/10ws-sem-mobsec/talks/dammann.pdf

How to Build Your Own Rogue GSM BTS for Fun and Profit
(Simone Margaritelli)
https://www.evilsocket.net/2016/03/31/how-to-build-your-own-rogue-gsm-bts-for-fun-and-profit

Building a portable GSM BTS using the Nuand bladeRF, Raspberry Pi and YateBTS (The Definitive and Step by Step Guide)
(strcpy)
https://blog.strcpy.info/2016/04/21/building-a-portable-gsm-bts-using-bladerf-raspberry-and-yatebts-the-definitive-guide

mindthesec 2016

OBRIGADO!

Igor Marcel e Wilberto Filho

igor@blazeinfosec.com | wilberto@blazeinfosec.com

@blazeinfosec

www.blazeinfosec.com

MAIS UM EVENTO: Flipside SECURITY BEYOND TECHNOLOGY