Безопасность беспроводных сетей Wi-Fi

Докладчик:
Саранчин Виталий Валерьевич

Wireless Fidelity

Является торговой маркой Альянса Wi-Fi, созданного в 1999 году

Не является техническим термином

Объединяет множество стандартов IEEE 802.11

Продукция, прошедшая сертификацию, может носить этот логотип и знак «Wi-Fi CERTIFIED»

http://wi-fi.org/

IEEE = IRE — Institute of Radio Engineers (1912) + AIEE — American Institute of Electrical Engineers (1884)

Institute of Electrical and Electronics Engineers
(Институт инженеров по электротехнике и электронике) — международная некоммерческая ассоциация специалистов
в области техники, мировой лидер в области разработки стандартов по радиоэлектронике и электротехнике.

Дата основания:	1 января 1963 года
Количество членов:	более 395 тысяч
Число стран-участников:	более 160 (45% за пределами США)

http://www.ieee.org/

Семейство стандартов IEEE 802.11

IEEE 802.11

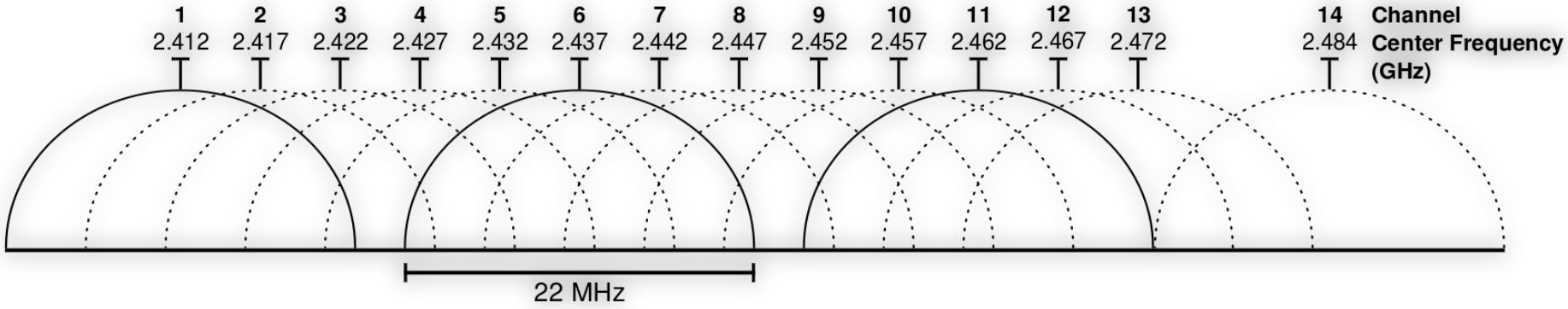
множество стандартов WLAN (беспроводной локальной сети)
в диапазонах частот 2,4, 3,6 и 5 ГГц

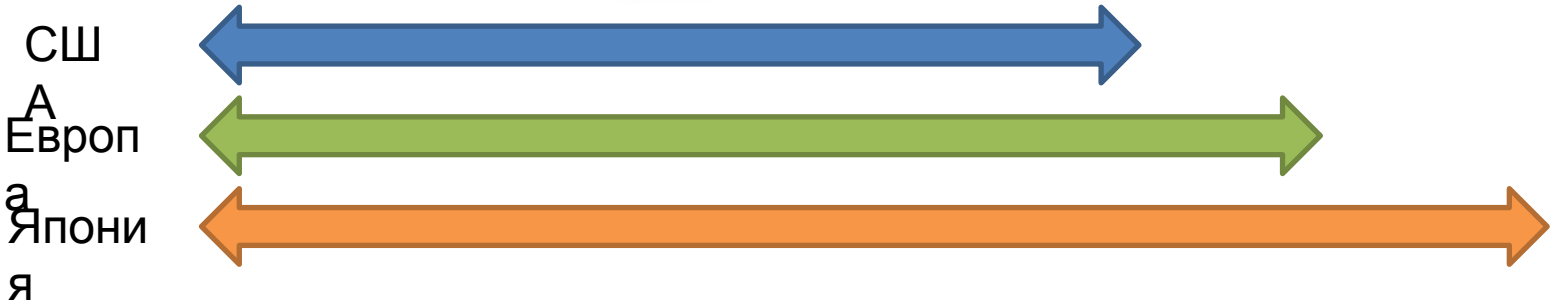
Поддерживается комитетом стандартов IEEE 802

Стандарт 802.11	Год	Частота (ГГц)	Максимальная пропускная способность
	1997	2.4	2 Мбит/с
a	1999	5.0	54 Мбит/с
b	1999	2.4	11 Мбит/с
g	2003	2.4	54 Мбит/с
n	2009	2.4 / 5.0	480 Мбит/с

Текущая базовая версия стандарта: IEEE 802.11-2007

Распределение частот по индивидуальным каналам в диапазоне 2.4 ГГц





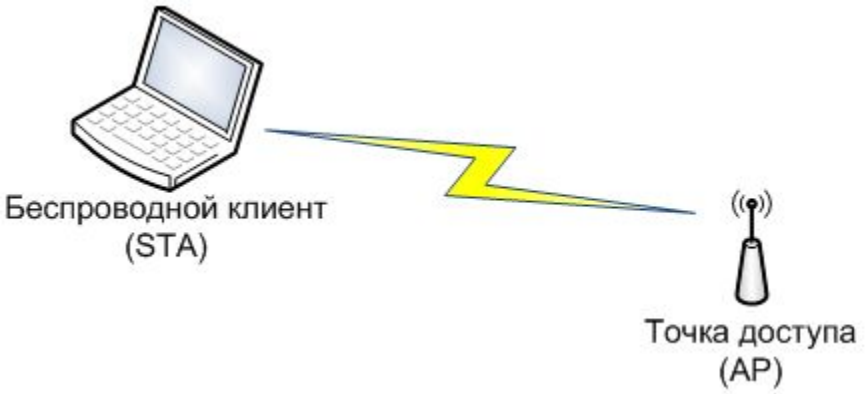
Количество неперекрывающихся каналов мало

При работе на соседних каналах устройства могут оказывать
влияние друг на друга, создавая помехи

Основные режимы работы сетей Wi-Fi

- **Infrastructure**
- **IBSS (Independent Basic Service Set)**
- **WDS (Wireless Distribution System)**

Схема типичной инфраструктурной сети 802.11b/g



SSID	• Имя сети, содержит до 32 символов
BSSID	• MAC-адрес точки доступа
Номер канала	• 1—13
Скорость передачи	• До 54 Мбит/с
Тип шифрования	• OPN, WEP, WPA, WPA2
Ключевой алгоритм	• OPN, WEP, TKIP, CCMP
Тип аутентификации	• OPN, PSK, 802.1X

Что нужно знать о сети Wi-Fi

?

Открытые сети Wi-Fi (без шифрования)

Преимущества

- Простота настройки
- Скорость работы сети в этом режиме максимальная

Недостатки

- Свободный доступ к сети для посторонних
- Возможность прослушивания передаваемых данных

Способы устранения проблем

- Отключение вещания SSID — малоэффективно, потому что на запрос клиента он передается в открытом виде
- Контроль доступа по MAC-адресам клиентов — также малоэффективная мера (MAC-адрес относительно легко подделать)
- Шифрование всего трафика внутри сети с помощью различного рода VPN — единственная действенная мера

Шифрование WEP (Wired Equivalent Privacy)

Информация

- Представлен как часть стандарта IEEE 802.11 в 1997 году
- Является устаревшим и не рекомендуется к использованию
- Возможно несколько видов атак на WEP

Особенности шифрования

- Использует ключи длиной 40 или 104 бит (некоторые производители могут использовать длину ключей 128, 256 бит)
- Основан на поточном шифре RC4, имеющем уязвимые места, и алгоритм CRC-32 для проверки

Известные типы атак на WEP

- **Fluhrer, Mantin, Shamir (2001**) — требует наличия слабых IV, необходимо перехватить около 500 тыс. таких кадров
- **KoreK («Chopchop») (2004)** — требуется перехватить несколько сотен тысяч кадров, не обязательно со слабыми IV. Для анализа используются только IV.
- **Tews, Weinmann, Pyshkin (2007)** — возможность инъекции ARP-запросов в сеть, что значительно ускоряет атаку. Необходимо перехватить несколько десятков тысяч кадров

Методы решения проблемы

- Использование туннелирования, например, IPSec
- Использование дополненных производителями стандартов: WEP 2, WEP Plus, Dynamic WEP
- Использование IEEE 802.11i (WPA/WPA2)

Wi-Fi Protected Access (WPA)

Информация

- Реализует основную часть протокола IEEE 802.11i
- Создавался в качестве замены WEP и являлся переходным этапом на пути к полной реализации IEEE 802.11i (WPA2)
- Возможно несколько типов атак на WPA

Особенности шифрования

- Использует **TKIP** (Temporal Key Integrity Protocol) или **CCMP** (**C**ounter Mode with **C**ipher Block Chaining **M**essage Authentication Code **P**rotocol) на базе AES
- Использует 256-битный ключ (64 шестнадцатеричные цифры) либо парольную фразу от 8 до 63 печатаемых ASCII символа
- В режиме PSK использует алгоритм PBKDF2 для получения ключа из пароля (SSID в качестве соли и проход 4096 циклов HMAC-SHA1)

Wi-Fi Protected Access (WPA)

Типы атак

- Перебор методом грубой силы (**Bruteforce**) или атака по словарю (**Dictionary attack**)
- **Tews—Beck (2008)** — основана на уязвимости WEP, что позволяет расшифровать короткие пакеты (ARP). Требует включенного QoS (802.11e). Атака позволяет получать ключевой поток отдельного пакета и использовать его семикратно для инъекции пакетов такой же длины в сеть (например, для спуфинг-атаки)
- **Ohigashi—Morii (2009)** — для атаки не требуется наличие QoS
- **Tews (2010)** — позволяет расшифровать весь трафик к клиенту

Методы решения проблем

- Использование стойкой парольной фразы
- Отключение QoS, установка времени смены ключей при использовании TKIP < 60 с
- Переход на использование WPA2
- Использование EAP-расширений протокола (сервер 802.1X)

Wi-Fi Protected Access (WPA2)
IEEE 802.11i-2004

Информация

- Реализует основную часть протокола IEEE 802.11i
- Наиболее надежный метод защиты беспроводной сети
- Рекомендуется к использованию взамен устаревших WEP и WPA

Особенности шифрования

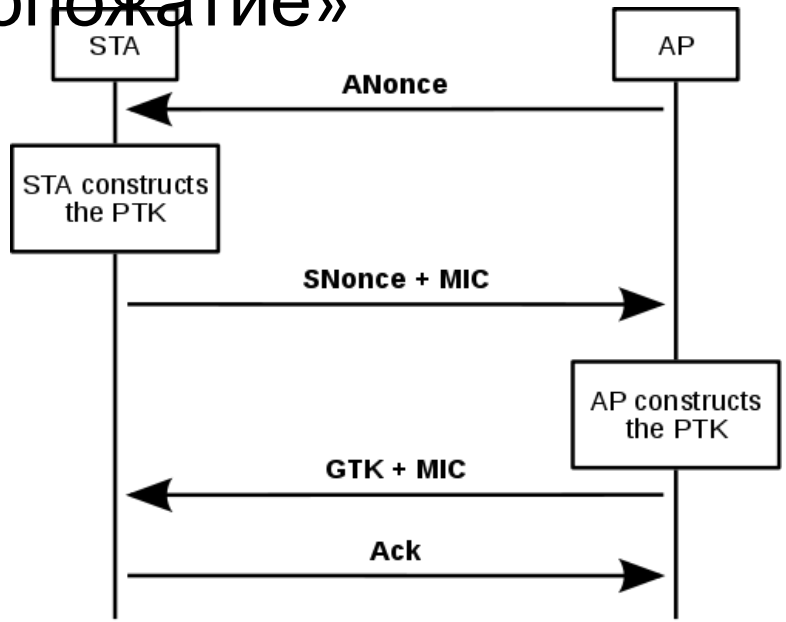
- Использует только **CCMP** на базе AES
- Может использоваться режим PSK или EAP

Методы атаки

- Перебор методом **Bruteforce** или **Dictionary attack**

Для ускорения перебора паролей используются технологии CUDA и ATI Stream,
задействующие мощности GPU, а также Rainbow Tables. Необходим перехват
четырехступенчатого «рукопожатия».

Четырехступенчатое «рукопожатие»



PTK — Pairwise Transient Key (парный промежуточный ключ)
MIC — Message Integrity Code (код целостности сообщения)
GTK — Groupwise Transient Key

Инструменты для анализа безопасности сетей 802.11

Информация

- Дистрибутив **BackTrack** сделан на основе Ubuntu и является одним из лучших наборов инструментов по тестированию безопасности на сегодняшний день
- Последняя доступная версия — BackTrack 4 R2 (дата релиза — 22 ноября 2010

Преимущества дистрибутива

- Поддержка множества беспроводных адаптеров
- Бесплатное распространение BackTrack
- Наличие множества дополнительных инструментов на любой вкус
- Активное развитие проекта

Инструменты, используемые в демонстрации WEP

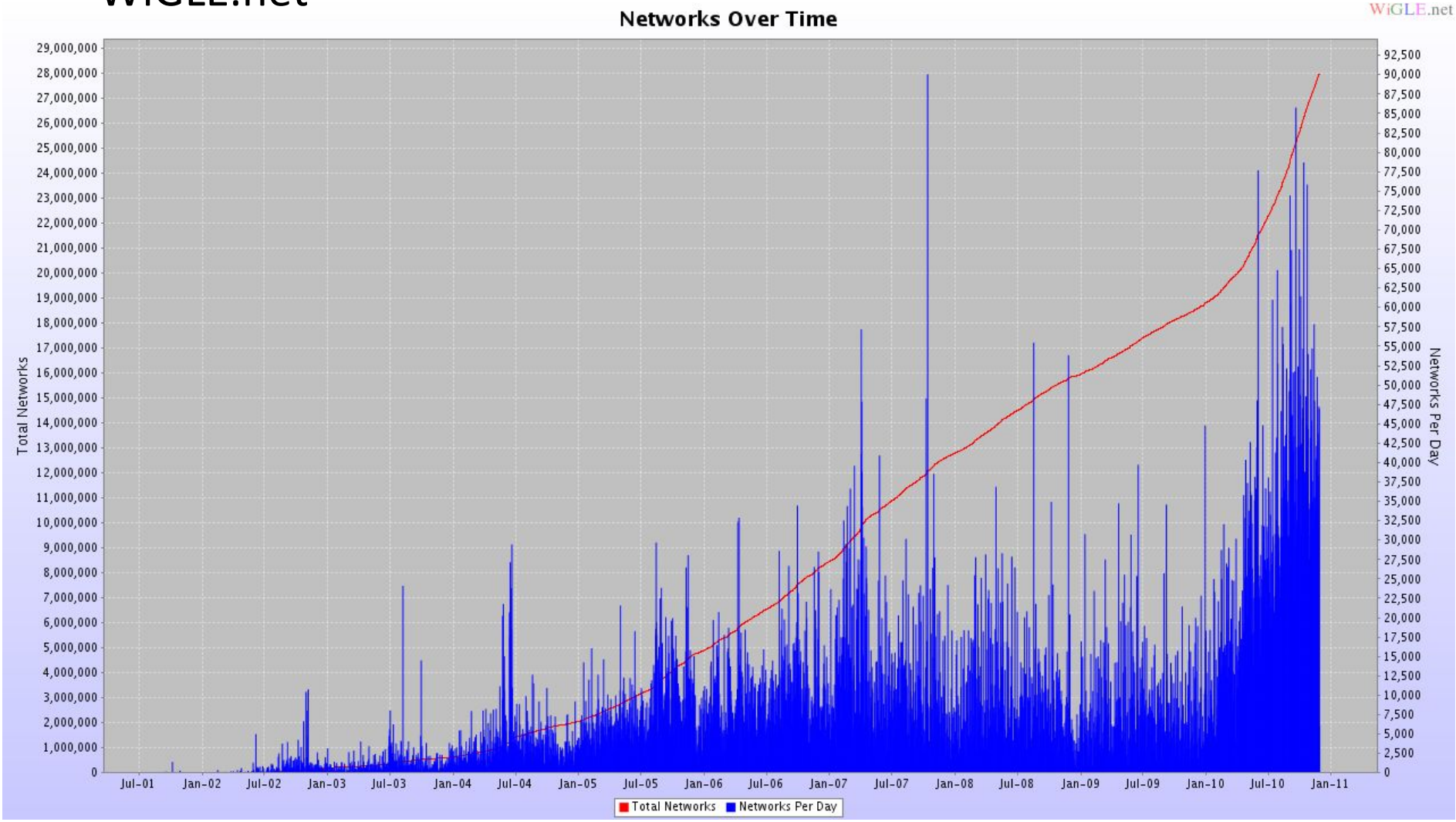
- Aircrack-ng

Инструменты, используемые в демонстрации WPA

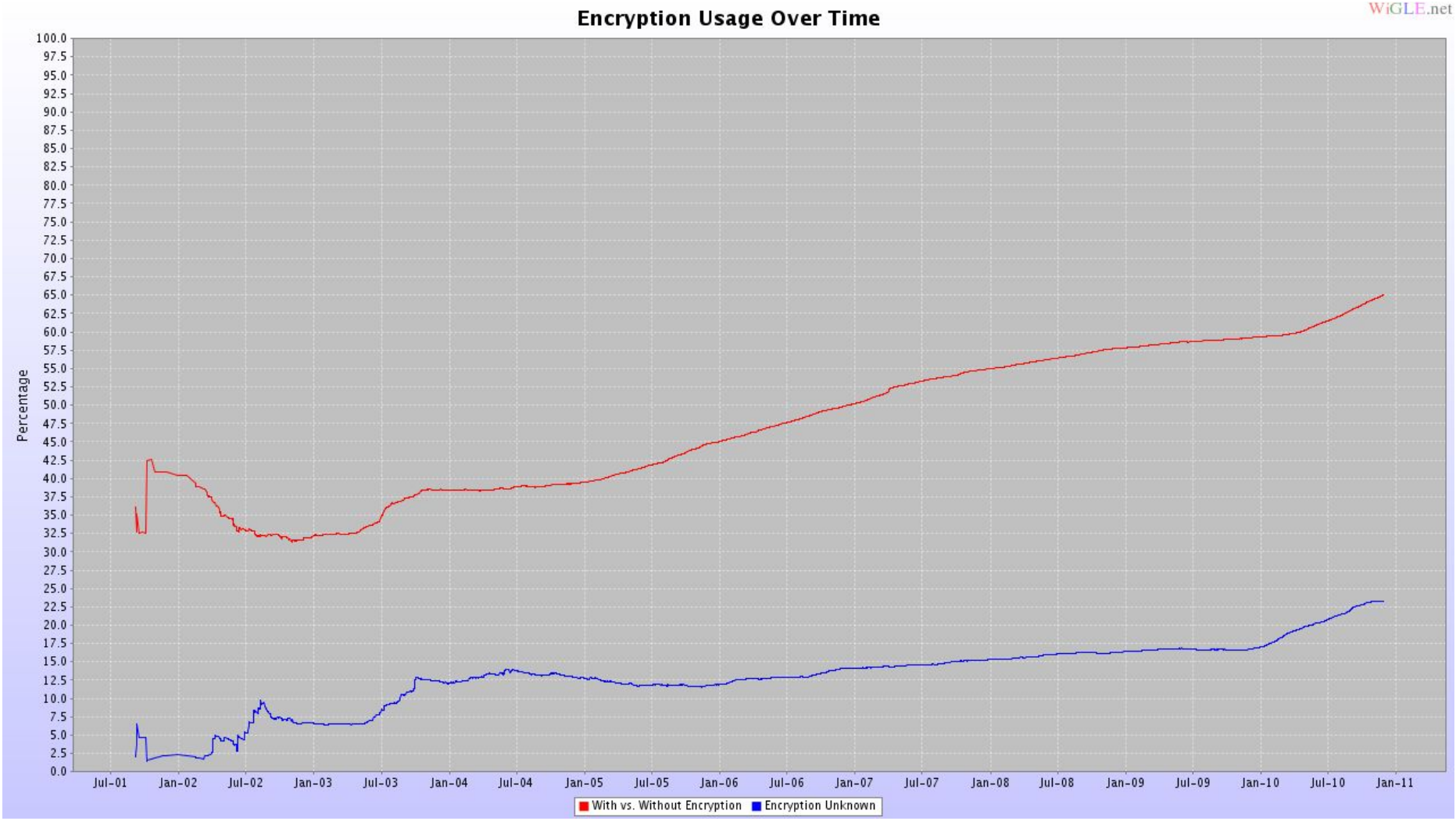
- Aircrack-ng
- Pyrit
- coWPAtty

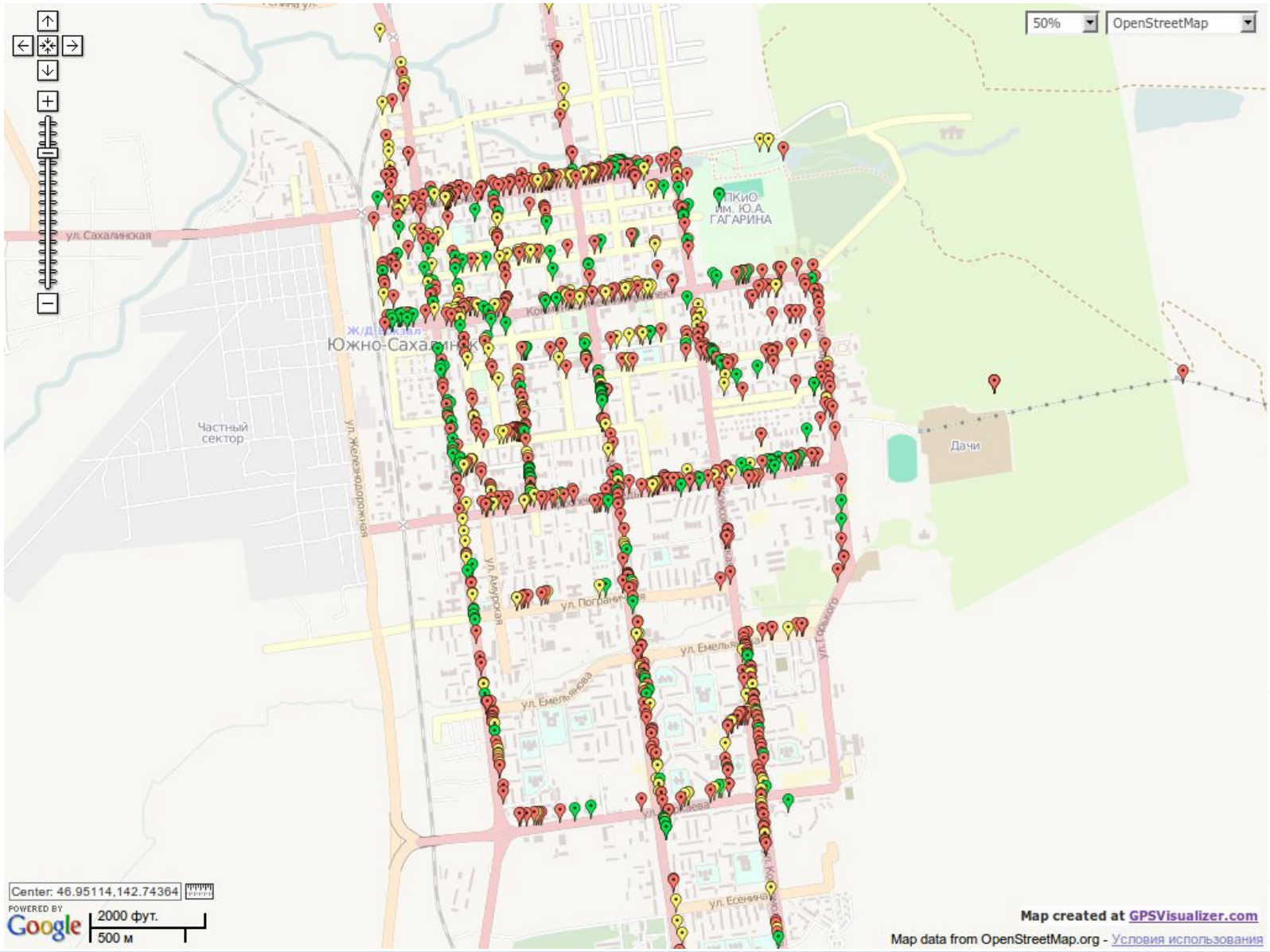
http://www.backtrack-linux.org/

Статистика по количеству беспроводных сетей на WiGLE.net



Статистика по использованию шифрования на WiGLE.net




50%
OpenStreetMap
ул. Сахалинская
ЦПКиО им. Ю.А. ГАГАРИНА
Южно-Сахалинск
Частный сектор
ул. Железнодорожная
ул. Амурская
ул. Пограничная
ул. Емельянова
Дачи
Center: 46.95114,142.74364
POWERED BY Google
2000 фут.
500 м
Map created at GPSVisualizer.com
Map data from OpenStreetMap.org - Условия использования

IT.conf_2010

Схема демонстрационной