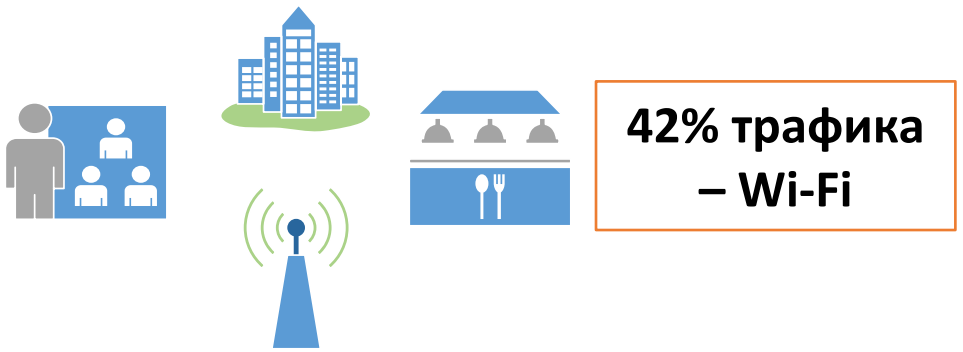
ООО «НеоБИТ»

ЗАЩИТА БЕСПРОВОДНЫХ КЛИЕНТОВ ОТ АТАК, ОСНОВАННЫХ НА ИСПОЛЬЗОВАНИИ ОСОБЕННОСТЕЙ ПОСТРОЕНИЯ WI-FI-СЕТЕЙ

Зегжда Д.П., Москвин Д.А., Дахнович А.Д.

РусКрипто 2017

Актуальность проблемы безопасности беспроводных сетей



42% трафика – Wi-Fi

25% Wi-Fi точек не защищены

80% точек имеют пароли по умолчанию

3% точек защищены Протоколом WEP

Результат

77% пользователей публичных Wi-Fi подвергались кибератакам

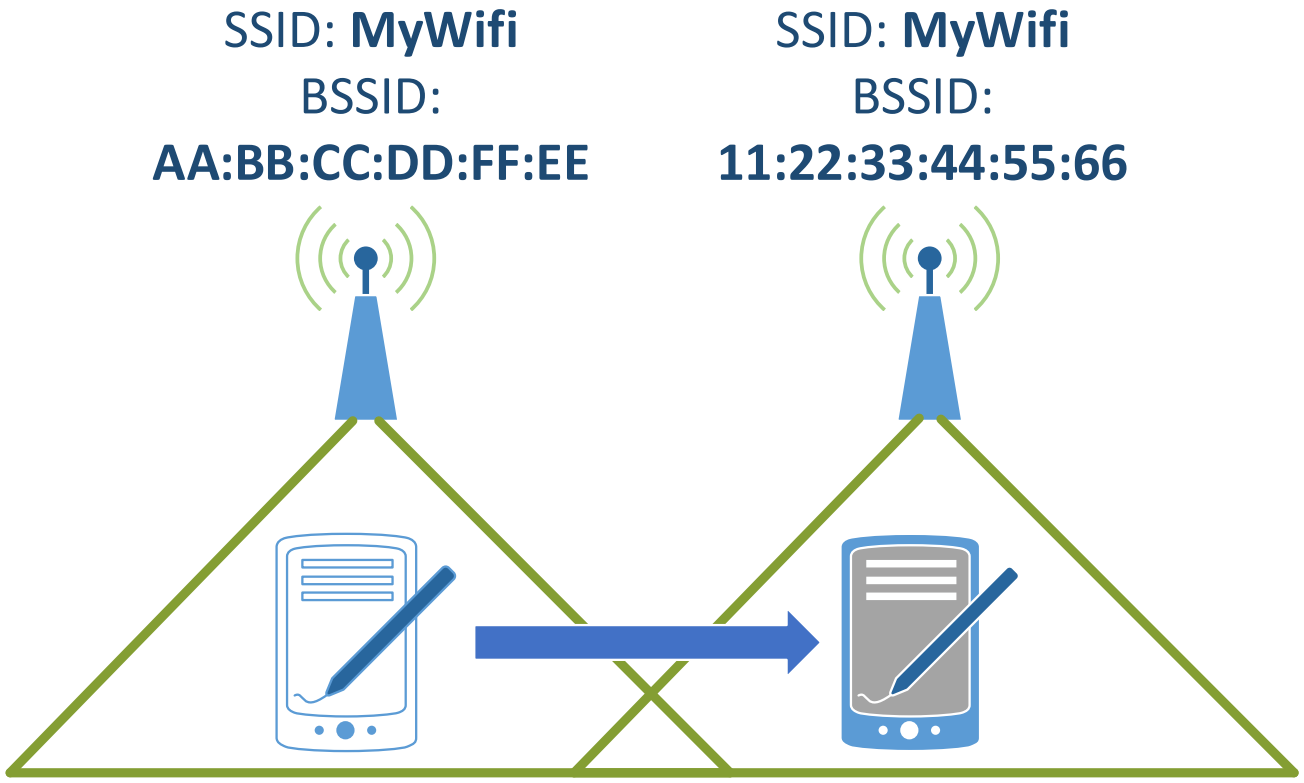
Анализ существующих механизмов обеспечения безопасности Wi-Fi сетей

Тип сети / Мера защиты	Открытая сеть	WEP	WPA2 Персональный	WPA2 Предприятия
Тип аутентификация	-	Общий ключ	Общий ключ	Персональные данные
Аутентификация клиента	-	+	+	+
Аутентификация сети	-	-	-	+/- (зависит от метода аутентификации)
Использование сервера аутентификации	-	-	-	+

Роуминг между точками доступа

Основные причины:

- сигнал от ТД становится хуже порогового значения;
- отношение мощности сигнала к шуму;
- множество повторных отправок пакетов;
- прямое отсоединение пакетами деаутентификации.



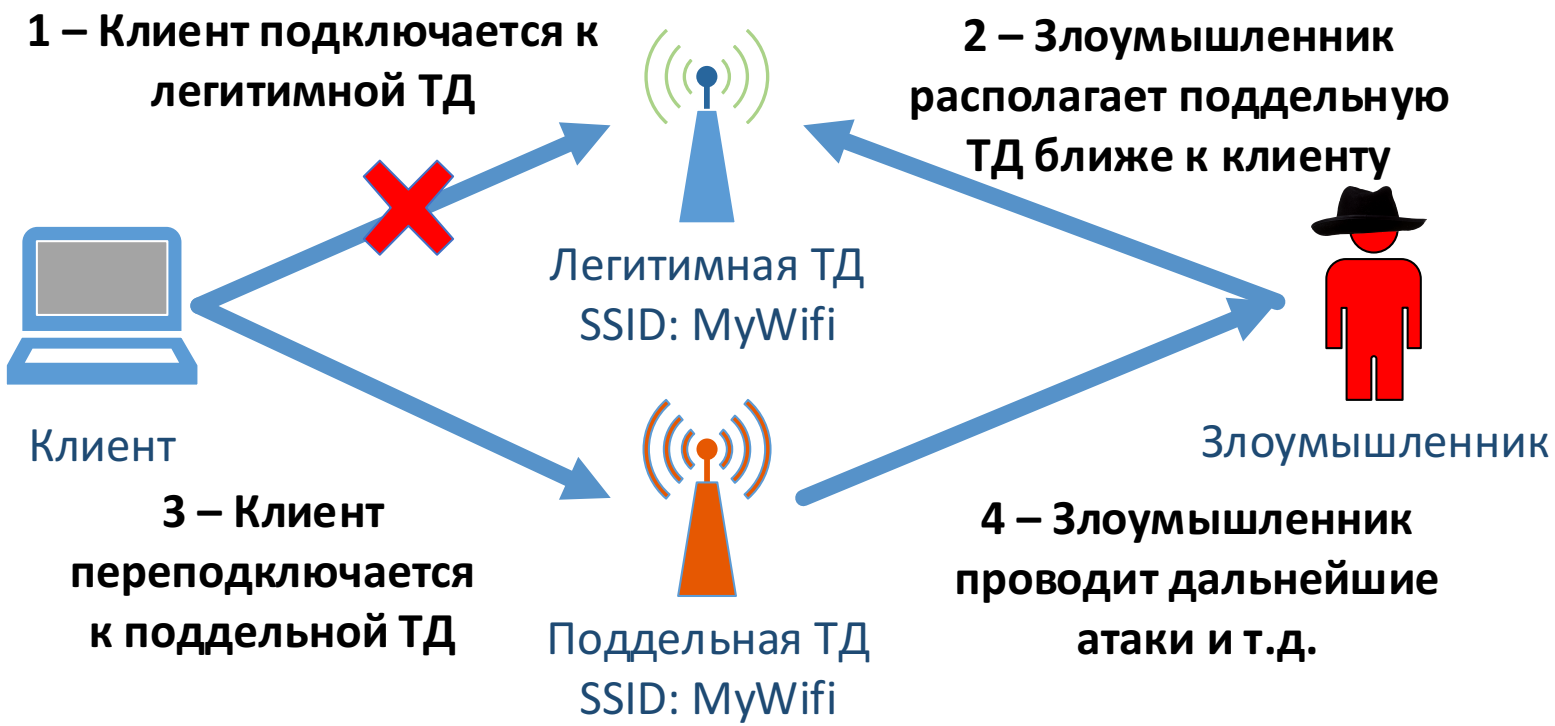
Атака поддельной ТД

Сценарий атаки

Злоумышленник устанавливает вблизи жертвы ТД и переподключает к ней устройство клиента.

Условие

На устройстве клиента сохранена сеть с данной SSID



Сложность проведения атаки в зависимости от протокола безопасности

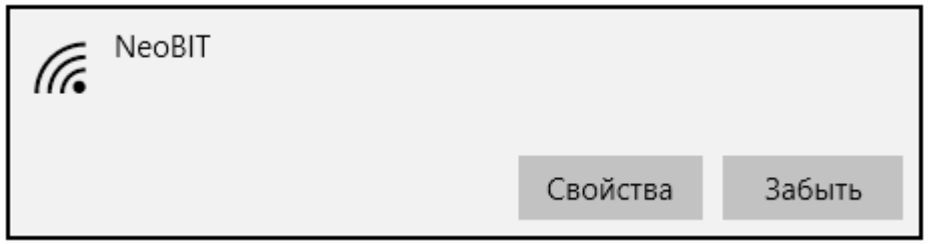
Условие / Тип сети	Знание SSID	Знание общего ключа	Наличие сервера аутентификации	Трудоемкость проведения атаки
Открытая сеть	+	-	-	-
WEP	+	+	-	-
WPA2 Personal	+	+	-	+
WPA2 Enterprise	+	-	+	++

Существующие средства защиты от поддельных ТД на стороне сервера

На стороне сети (только корпоративной) – WIPS:

- установка ТД-детекторов;
- ведение списков.

На стороне клиента



1. Предотвращение подключения:
   - каждый раз «забывать сеть»
   - фильтры, стороннее ПО (WIPS на клиенте)
   - подключаться только к WPA2 с 802.1X
   - отключать беспроводной адаптер
2. Постзащита: VPN, HTTPS Everywhere

Сравнение средств и методов защиты в точки зрения сценариев атаки поддельных ТД

Ср-ва и методы / Сценарий атаки	WIPS	«Забыть сеть»	Стороннее ПО и фильтры	Только 802.1X сети	VPN/HTTPS
Подключение клиента к той же сети	+	+	+	+/-	+/-
Подключение ассоц. клиента к другой сети	-	-	-/+	+	+/-
Подключение неассоц. клиента к сети	-	+	-/+	+/-	+/-
Подключение клиента по перебору сети	-	-	-	+/-	+/-

Разработанная схема аутентификации ТД

Реализация разработанной схемы

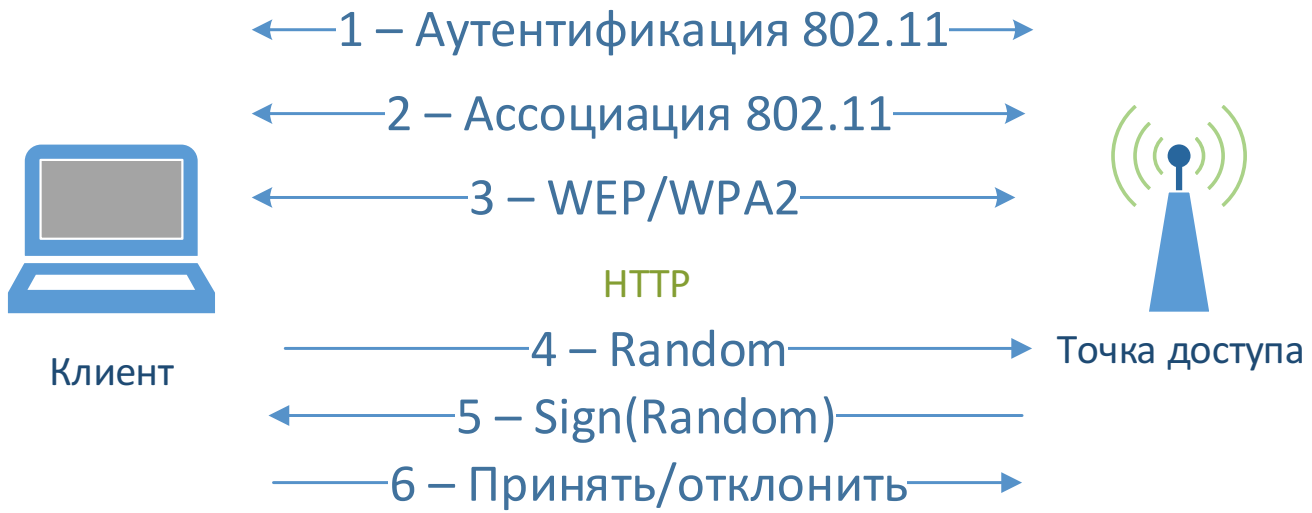
через TCP-сокеты или веб-сокеты

Преимущества:

- простота реализации;
- не нужно вносить изменения в стандарт.

Недостатки:

- не универсально;
- нужно контролировать доступ к сети.



Преимущества разработанной схемы

1. Защита от сценариев атаки поддельных точек доступа.
2. Поддержка автоматического подключения к аутентифицированным ТД.
3. Возможность распространение схемы аутентификации для защиты от поддельных клиентов.
4. Реализация на различных уровнях модели OSI (канальный, сетевой, прикладной).