Методы обеспечения безопасности при обнаружении соседей

Обзор уязвимостей и некоторых методов защиты в протоколах обнаружения соседей

Протоколы ND

- Обнаружение маршрутизаторов и префикса подсети (Router and prefix discovery)
- Разрешение адресов и обнаружение недостижимости (Address resolution and neighbor unreachability detection)
- Перенаправление (Redirect)

Протоколы AAC

- Обнаружение дубликатов адреса (Duplicate address detection)
- Выделение глобальных и локальных адресов (Creation of global and site-local addresses)

Сообщения

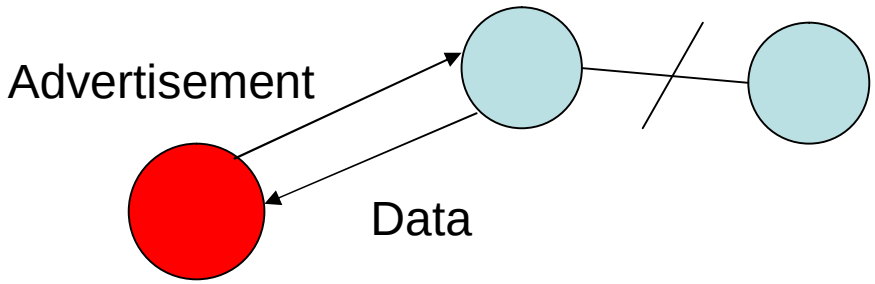
- Router solicitation
- Router advertisement
- Neighbor solicitation
- Neighbor advertisement
- Redirect
- Сообщения могут передаваться как в режиме Unicast, так и в режиме Multicast.

Уровни безопасности сегментов сети

- Корпоративная сеть
  Физическое подключение новых узлов затруднено
- Сеть с оператором
  В сегменте имеется маршрутизатор провайдера, которому можно доверять
- Одноранговая сеть
  Анархия

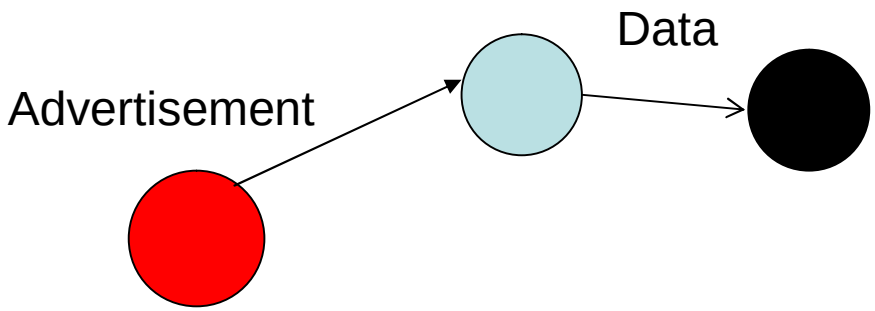
Возможные атаки 1

- Подделка пакетов Neighbor Solicitation и Neighbor Advertisement.
  Может приводить к изменению кэша соседей и перенаправлению трафика на неправильный физический адрес. Один из способов защиты – криптографически связать физический адрес и IPv6 адрес.



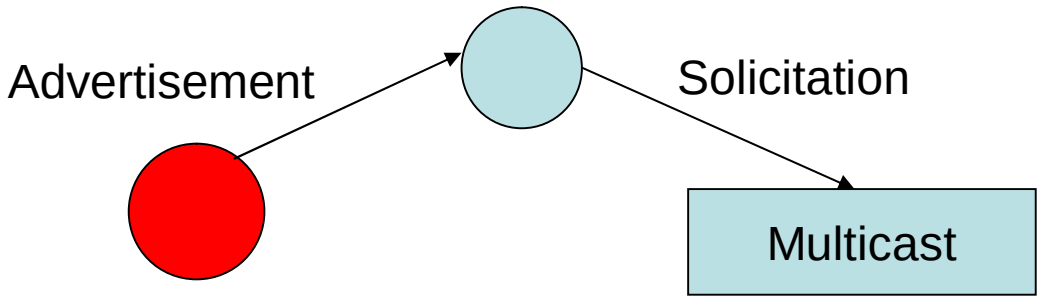
Возможные атаки 2

- Ошибка при проверке доступности соседа
  С помощью подделки пакетов Neighbor Advertisement злоумышленник может ввести в заблуждение свою жертву о доступности соседа, который уже не доступен



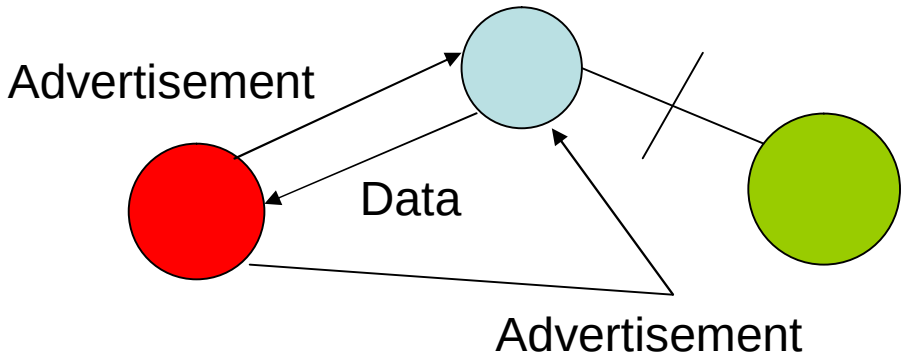
Возможные атаки 3

- Атака при проверке адреса на уникальность
  Злоумышленник может отвечать на все запросы Neighbor Solicitation, блокируя выделение новых адресов. Одно из решений – ограничить количество выделенных узлу адресов



Возможные атаки 4

- Ложный маршрутизатор
  Злоумышленник может посылать сообщения Router Advertisement, заявляя себя маршрутизатором. Чтобы подавить настоящий маршрутизатор, он может также посылать сообщения от его имени с нулевым временем жизни.

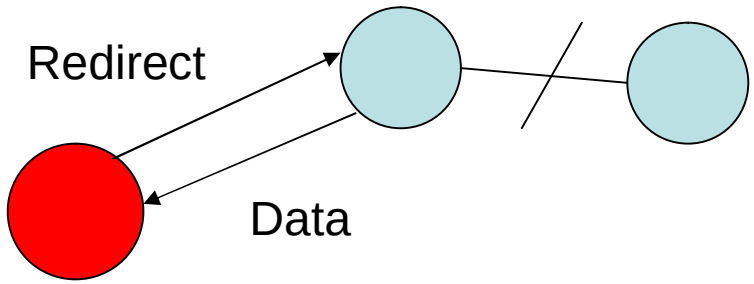


Возможные атаки 5

- Подавление всех маршрутизаторов
  Если злоумышленник подавит все маршрутизаторы, то он сможет выдавать себя за любой узел Интернета, т.к. при отсутствии маршрутизаторов считается, что все адреса находятся в локальном сегменте.

Возможные атаки 6

- Подделка перенаправления
  Злоумышленник может посылать пакеты Redirect от имени маршрутизатора, перехватывая трафик, предназначенный другому узлу или вызывая отказ в обслуживании.



Возможные атаки 7

- Подделка префикса локального сегмента

  Злоумышленник может послать сообщение Router Advertisement, в котором будет указан произвольный префикс локального сегмента сети. В результате все хосты сегмента будут использовать ND для доступа к узлам этого префикса, что приведет к отказу или перехвату трафика.

Возможные атаки 8

- Подделка префикса для автоматической настройки адресов
  Злоумышленник может послать пакет Router Advertisement с неправильным префиксом для автоматической настройки адресов, что приведет к отказу в обслуживании или перехвату части трафика узлов, использовавших этот префикс для настройки.

Возможные атаки 9

- Подделка параметров
  Рассылка Router Advertisement с другими некорректными параметрами (например, Current Hop Limit) может приводить к отказу в обслуживании. Для защиты от этой атаки необходимо проверять параметры на корректность.

Возможные атаки 10

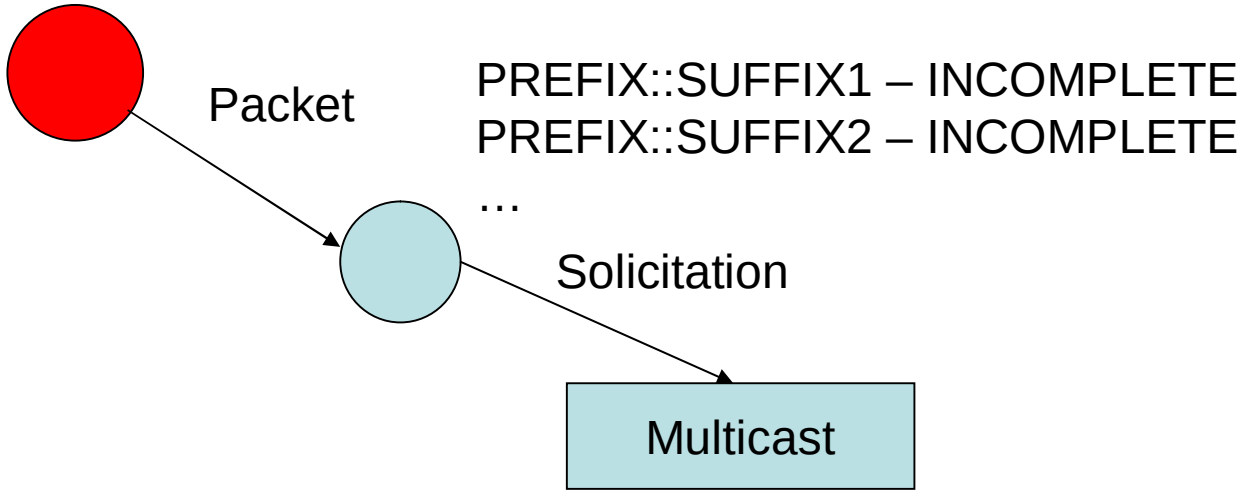
- Повторная передача пакетов
  Даже если данные шифруются, их можно перехватить и повторно передать. Для защиты можно использовать метку времени или уникальный код в паре запрос-ответ.

Удаленная атака

- Переполнение кэша маршрутизатора
  Эта атака может быть выполнена удаленно. Злоумышленник посылает пакеты с правильным префиксом, но неправильным суффиксом. Маршрутизатор сегмента пытается использовать запрос Neighbor Solicitation для получения физического адреса узла, при этом занимается строка таблицы кэша. Если таких пакетов будет много, таблица может переполниться, что приведет к отказу в обслуживании.

Удаленная атака

- Методом борьбы с этой атакой может быть ограничение частоты попыток обнаружить нового соседа, запоминание локальных узлов на маршрутизаторе при их регистрации, более сложные алгоритмы кэширования.



Заключение

- Протоколы обнаружения соседей имеют уязвимости, следовательно их необходимо защищать.
- Использование IPsec не всегда удобно.
- Другие механизмы защиты существуют, но не для всех видов атак.