ПОЛИТЕХ
Санкт-Петербургский
политехнический университет
Петра Великого

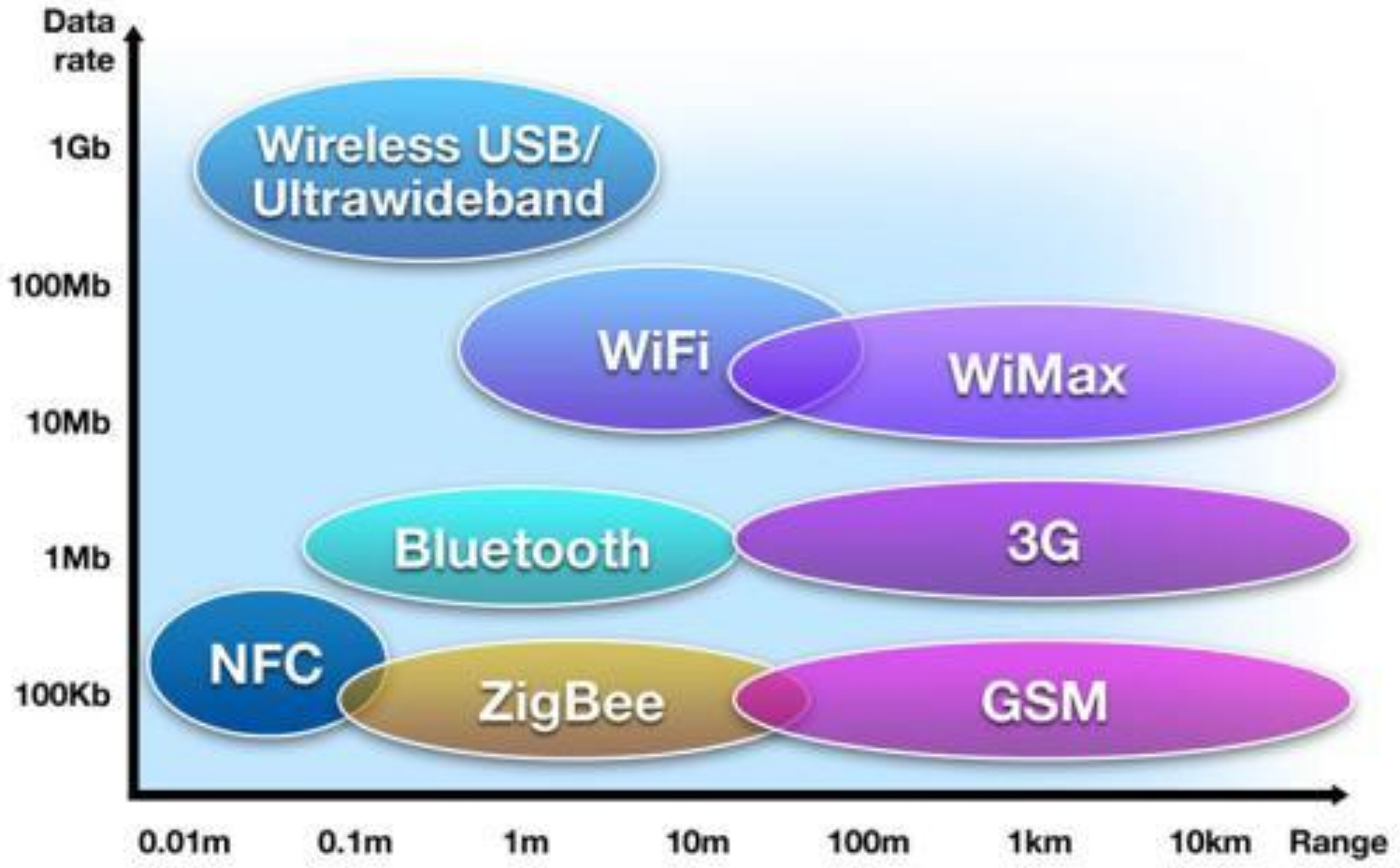
АНАЛИЗ БЕЗОПАСНОСТИ ТЕХНОЛОГИИ NFC ПРИ РЕШЕНИИ ПРИКЛАДНЫХ ЗАДАЧ

Мясников А.В.
аспирант
СПбПУ ИБКС

Технология NFC

- NFC = **N**ear **F**ield **C**ommunication
- Технология ближнего взаимодействия
  - Рабочая частота 13.56 Mhz
  - Основана на технологии RFID
  - Скорость передачи данных до 424 кбит/с (106, 212 кбит/с)
  - Быстрое время установки канала передачи данных (t < 0.1c)
  - Не требует «прямой видимости» между взаимодействующими устройствами
  - Очень низкое энергопотребление

Сравнение NFC с другими беспроводными технологиями передачи данных



Физическая схема взаимодействия

- Индуктивная связь
- Амплитудная модуляция
- OOK (**O**n-**O**ff-**K**eying) с различной глубиной модуляции

Режимы работы устройств

Устройство 1	Устройство 2	Описание
Активное	Активное	Поочередная генерация РЧ-поля каждым устройством
Активное	Пассивное	Устройство 1 генерирует РЧ-поле
Пассивное	Активное	Устройство 2 генерирует РЧ-поле
Пассивное	Пассивное	Взаимодействие неосуществимо

Применение технологии NFC

- Взаимодействие электронных устройств
  - Обмен данными
  - Сопряжение устройств
- Идентификация
  - Скидочные карты
  - Карты для контроля доступа
- Мобильная оплата
  - Бесконтактные платежи
  - Билеты на мероприятия

Применение технологии NFC

Сопряжение мобильных устройств

P2P

Умные «Плакаты»

Умные замки

Оплата

Безопасность NFC

Атаки на беспроводные каналы	Актуальность для NFC	Способ защиты
Пассивная прослушка	+	Криптография
Повреждение данных	+	Криптография + атаки обнаруживаются устройствами
Модификация данных	Атака реализуема, но с существенными ограничениями	Криптография
Вставка данных	Атака реализуема, но с существенными ограничениями	Криптография
Relay-атаки	+	Экранирование, подтверждение пользователя при передаче, использование Distance-Bounding протоколов криптографии
MITM-атаки	-	-

Пассивная прослушка канала

- Возможна с расстояния до 10 метров
- Съем с помощью направленной антенны
- Использование шифрования позволяет избежать атаки

Повреждение передаваемых данных

- Аналог атаки типа «отказ в обслуживании»
- Засорение канала передачи данных случайными данными
- Атаку легко отследить из-за всплесков мощности, создаваемых полем злоумышленника

Модификация передаваемых данных

- Зависит от схемы кодирования и коэффициента модуляции
  - Инвертируются все биты
  - Инвертируются 1 на 0, в случае, если перед битом стояла 1.
- В качестве защиты можно использовать криптографические методы
- Существует возможность обнаружения РЧ-поля злоумышленника в момент передачи

Атака вставки данных

- Посылка ответа раньше легитимного устройства
- В качестве защиты:
  - Криптографические средства защиты
  - Прослушка канала вторым устройством во время передачи, с целью выявления злоумышленника
  - Использование предвычислений для ускорения ответа

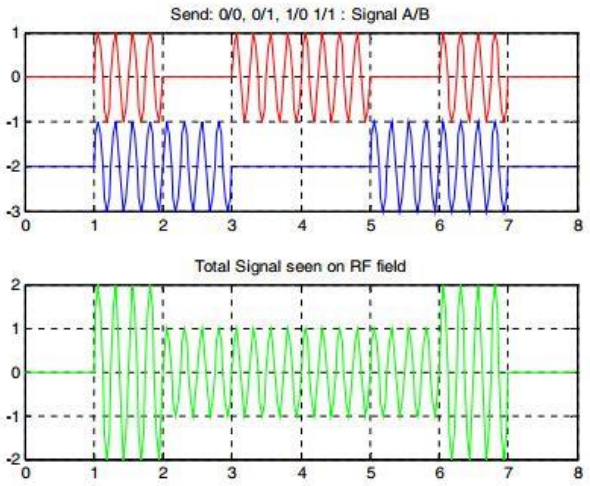
Relay-атаки

- «Увеличение» радиуса действия источника NFC-сигнала засчёт съёма сигнала легитимного устройства и пересылки его по побочному каналу
- Методы защиты:
  - Экранирование
  - Distance-bounding Protocols
  - Требование дополнительных активных действий от пользователя

MITM-атаки

- Для любых конфигураций общающихся устройств можем обнаружить атаку и прекратить обмен информацией
- Для конфигурации «активное-активное» не можем послать сообщение только одному адресату
- Для «пассивное-активное» не сможем идеально подобрать оба поля, чтобы не исказить сообщения

Специфичный для NFC алгоритм установки сеансового ключа



	0	1
0	Отбрасываем	Принимаем
1	Принимаем	Отбрасываем

- Низкая вычислительная сложность
- Оба устройства синхронизированы и посылают случайные данные в канал
- Новый бит выбирается с вероятностью 50%

Перечень рекомендаций для обеспечения безопасного канала передачи данных по NFC

- Использование шифрования
- Экранирование устройств
- Distance-bounding протоколы
- Подтверждение передачи

Прототип системы синхронизации пользовательских данных с установкой безопасного канала по NFC