УДК 004.056

Анализ безопасности NFC при использовании в мобильных устройствах

Смирнов А.Г.
(Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, г. Санкт-Петербург)

Научный руководитель – к.т.н., доцент Волошина Н.В.
(Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, г. Санкт-Петербург)

Аннотация: В работе проводится исследование технологии NFC, её характеристик и варианты применения, а также рассмотрены некоторые аспекты её безопасности.

На сегодняшний день технология NFC очень активно внедряется в смартфоны и планшеты, и большинство современных мобильных устройств уже оснащены NFC-модулями.

NFC имеет широкую область применения, и обусловлено это тем, что технология обладает большой функциональностью и относительно невысокой стоимостью. С помощью оснащенного NFC телефона можно взаимодействовать с бесконтактными метками, устанавливать связь с устройствами, у которых есть NFC модули, совершать покупки, оплачивать проезд в транспорте и многое другое.

В ходе работы:

- Рассмотрены основные аспекты информационной безопасности NFC
- Выявлены существующие угрозы NFC
  - Повреждение данных
    В этом случае атакующий может нарушить связь таким образом, что принимающая сторона будет не в состоянии корректно принять данные, посылаемые отправителем. Данную атаку относительно легко реализовать средствами РЭБ, то есть заглушить передачу и прием данных RFID. Предотвратить такую атаку достаточно сложно, но единственный ее результат – это невозможность установить соединение между отправителем и получателем.
  - Прослушивание
    В этом случае, например, злоумышленник может воспользоваться направленной антенной, чтобы попробовать подслушать передаваемую информацию. Таким образом может производиться перехват данных для дальнейшего клонирования или модификации.
  - Модификация данных
    Такая атака, как несанкционированное изменение данных в сообщении атакующим устройством, крайне труднореализуемая на практике в связи с особенностями работы NFC, то есть невозможностью предсказать амплитуду и сдвиг фазы наведенного сигнала на приемном устройстве. Однако при успешном перехвате, злоумышленник может подменить трафик данных.
  - Relay attack
    В этом случае атакующий должен отправить в реальный момент времени запрос считывателя, а ответ передать дальше на считывающее устройство. Это предпринимается, чтобы исполнить задачу по симуляции владения картой жертвы,

но реализация данной атаки достаточно трудна из-за сильного ограничения по времени на ответ запрашиваемого устройства.

- Определены способы защиты NFC

В результате работы для исследования уязвимостей реализовано приложение под ОС Android, взаимодействующее с NFC метками, было проведено исследование безопасности технологии NFC и выявлено, что существует проблема безопасности персональных данных. В своем исходном виде технология NFC не защищает пользователей от прослушивания трафика, то есть все данные передаются в открытом виде. Отсутствуют стандарты и протоколы для защиты передаваемых данных.