УДК 004.056
DOI 10.21685/2587-7704-2020-5-2-2

Open Access | RESEARCH ARTICLE

Анализ существующих угроз безопасности технологии NFC

А. В. Родин
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

Аннотация. Рассматриваются существующие угрозы информационной безопасности технологии NFC, описывается их реализация, приводятся некоторые методы защиты.

Ключевые слова: технология NFC, угроза информационной безопасности, атаки на технологию NFC.

Analysis of existing security threats to NFC technology

A. V. Rodin
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

Abstract. The article describes the existing threats to information security of NFC technology. The main types of attacks against NFC technology are given, and some protection methods are considered.

Keywords: NFC technology, information security threat, attacks against NFC technology.

Near Field Communication (NFC), связь ближнего действия – технология беспроводной передачи данных малого радиуса действия, обеспечивающая возможность передачи данных между устройствами, расположенными на расстоянии до 10 см.

В настоящее время темп распространения технологии NFC по различным областям жизнедеятельности человека крайне высок, и уже сейчас рассматриваемая технология применяется в следующих областях [1]:

– платежные системы;
– системы контроля и управления доступом;
– обмен информацией между устройствами;
– благоустройство и цифровизация городов;
– транспортная сфера;
– сфера здравоохранения;
– контроль подлинности изделий.

Широкая область применения данной технологии делает ее уязвимой для различных типов атак, использующих различные имеющиеся уязвимости в различных областях применения.

В технологии NFC имеются два основных объекта – приемник и передатчик информации. В роли приемника выступают различные считывающие устройства, а в роли передатчика – пассивные устройства (карты, метки и в большинстве случаев смартфоны). Злоумышленником могут быть реализованы атаки как на принимающую сторону, так и на передающую [2].

В ходе изучения информации о технической реализации устройств, использующих NFC для работы, были выявлены существующие угрозы, направленные на активный обмен информацией между приемником и передатчиком:

1. Повреждение данных.
2. Прослушивание канала связи.
3. Модификация передаваемых данных.

4. Атака посредника.
5. Несанкционированное считывание информации.
6. Блокировка записи карты.
7. Изменение времени действия карты.

В табл. 1 приведены угрозы, реализуемые непосредственно в момент обмена информацией между считывателем и носителем. После определения существующих угроз были исследованы способы реализации каждой угрозы и последствия [3].

Таблица 1

Описание существующих угроз, направленных на канал связи

Номер угрозы	Описание реализации угрозы	Последствия реализации угрозы
1	Атакующая сторона с использованием средств радиоэлектронной борьбы имеет возможность сделать невозможным передачу и прием данных при помощи NFC	Невозможность установить контакт между принимающей и передающей сторонами
2	Атакующая сторона с помощью направленной антенны имеет возможность перехватить передаваемые данные	Передаваемые данные становятся известными нарушителю, который впоследствии сможет их использовать в своих целях
3	Атакующая сторона с помощью специальных технических средств имеет возможность перехватить данные и модифицировать их	Подмена передаваемого трафика
4	Атакующая сторона с помощью специальных технических средств имеет возможность имитировать действия передающей стороны для симуляции действия легитимной передающей стороны	Имитация действий легитимного пользователя может привести к нежелательным последствиям
5	Атакующая сторона с помощью специальных технических средств имеет возможность скрытно (незаметно для пользователя) считать информацию с карты пользователя	Компрометация данных, записанных на носителе
6	Атакующая сторона с помощью специальных технических средств имеет возможность перевести устройство пользователя в режим «только чтение» и заблокировать попытки записи информации считывателем	Карта становится доступной только для чтения, что может быть критичным в ряде случаев
7	Атакующая сторона с помощью специальных технических средств в том случае, когда срок действия карты прописан в метке, имеет возможность изменить метку времени	Карта может стать недоступной для выполнения операций, требующих метку времени карты

Необходимо отметить также и то, что большинство перечисленных угроз крайне труднореализуемы на практике по причине особенностей принципов функционирования NFC или же нейтрализуются путем применения организационных мер безопасности.

В табл. 2 приводится перечень видов атак на беспроводные каналы связи, их актуальность для NFC и способы защиты.

Таблица 2

Основные виды атак на беспроводные каналы связи, применимые в технологии NFC

Вид атаки	Актуальность для NFC	Способ защиты
Пассивное прослушивание передаваемых данных	Высокая	Криптографическая защита передаваемых данных обеспечит безопасную передачу по открытому каналу связи
Модификация передаваемых данных	Реализация атаки связана с существенными ограничениями	
Повреждение передаваемых данных	Высокая	
Дополнение передаваемых данных новой информацией	Реализация атаки связана с существенными ограничениями	
Несанкционированное пользователем подключение к устройству (relay-атаки)	Высокая	Организационные методы

Исходя из вышеперечисленного, для защиты от большей части атак служит криптография. Шифрование передаваемых данных защитит обе стороны взаимодействия от вмешательства, но будет

бесполезной в случае, когда злоумышленник будет намеренно повреждать передаваемую информацию или глушить радиочастотный канал связи. В случае с relay-атаками для защиты используются методы организационно-прикладного уровня:

– использование экранированных чехлов для хранения устройств, поддерживающих технологию NFC, позволит пользователю быть уверенным в том, что устройство используется только по необходимости и не реагирует на несанкционированные запросы;

– необходимость подтверждения пользователя при выполнении операций также защитит устройство от воздействия извне.

Кроме рассмотренных выше атак непосредственно на канал связи, существует тип атак, направленный на пассивное устройство, не участвующее в радиочастотном обмене информации в момент проведения атаки [4]:

1. Модификация (повреждение) хранимых данных.
2. Копирование хранимых данных.
3. Блокировка записи карты.
4. Изменение времени действия карты.

Описание атак на пассивные устройства приведено в табл. 3.

Таблица 3

Описание существующих угроз, направленных на пассивное устройство

Номер угрозы	Описание реализации угрозы	Последствия реализации угрозы
1	Атакующая сторона с помощью специальных технических средств имеет возможность изменить данные, хранимые на устройстве	Информация, хранимая на атакуемом устройстве, становится невалидной
2	Атакующая сторона с помощью специальных технических средств имеет возможность скопировать данные, хранимые на устройстве	Компрометация хранимой информации
3	Атакующая сторона с помощью специальных технических средств имеет возможность перевести устройство пользователя в режим «только чтение» и заблокировать попытки записи информации считывателем	Карта становится доступной только для чтения, что может быть критичным в ряде случаев
4	Атакующая сторона с помощью специальных технических средств имеет возможность изменить метку времени действия устройства (при ее наличии)	Устройство может стать недоступным для взаимодействия

В табл. 4 приводится перечень атак, направленных непосредственно на устройство хранения информации и способы защиты, применяемые для защиты.

Таблица 4

Основные виды атак на беспроводные каналы связи, применимые в технологии NFC

Вид атаки	Способ защиты
Модификация (повреждение) хранимых данных	Блокировка несанкционированной записи данных
Копирование хранимых данных	Использование криптографических методов защиты информации
Блокировка записи карты	Блокировка определенных команд от неразрешенного пользователя
Изменение времени действия карты	Блокировка несанкционированной записи данных

Рассматривая угрозы, направленные на пассивное устройство NFC, можно сделать вывод о том, что устройства, хранящие информацию, подвержены атакам, направленным на несанкционированное блокирование, изменение или копирование записанных данных. В настоящее время применяются следующие способы защиты от рассмотренных угроз:

– хранение данных в зашифрованном виде (проприетарные стандарты производителей, DES/AES шифрование);

– использование механизма аутентификации в секторе памяти для чтения/записи. Данный способ позволяет защитить устройство хранения данных от попыток несанкционированного чтения/записи;

– использование нескольких уровней безопасности позволяет контролировать возможность выполнения определенных команд, что дает возможность провести активацию карты и полностью заблокировать ее от дальнейших изменений.

В настоящее время отсутствуют утвержденные стандарты и протоколы для защиты передаваемых данных, и в обычном случае данные передаются в открытом виде, что делает технологию NFC в ее исходном виде непригодной для передачи персональных данных или информации ограниченного доступа. Для передачи информации перечисленных типов необходимо использовать дополнительные механизмы защиты информации. Для обеспечения безопасности передачи информации по радиочастотному каналу связи требуется использовать защищенные каналы связи.

После проведения анализа возможных угроз, реализуемых по отношению к устройству с поддержкой технологии NFC, можно сделать вывод о том, что большинство рассмотренных угроз являются труднореализуемыми и ресурсоемкими и нейтрализуются при помощи применения организационных мер обеспечения безопасности.

Библиографический список

1. TN1216 Technical note. ST25 NFC guide, 2016
2. Ковынев, Н. В. Угрозы и способы защиты RFID и NFC меток / Н. В. Ковынев // Приборостроение – 2017 : материалы 10-й Междунар. науч.-техн. конф. (1–3 ноября 2017 г., Минск, Республика Беларусь) / Белорусский национальный технический университет ; редкол.: О. К. Гусев [и др.]. – Минск : БНТУ, 2017. – С. 78–79.
3. Михайлов, Д. М. Исследование механизмов проведения атак на RFID-системы / Д. М. Михайлов, А. В. Стариковский // Научное творчество 21 века : материалы 2 Всерос. науч. конф. – Красноярск : Научно-инновационный центр, 2010. – С. 16–17.
4. Стариковский, А. В. Атаки на мобильные телефоны, использующие технологии NFC / А. В. Стариковский, А. В. Зуйков, М. С. Аристов, Д. А. Степаньян // Безопасность информационных технологий. – 2012. – № 2. – С. 60–64.

Образец цитирования:

Родин, А. В. Анализ существующих угроз безопасности технологии NFC / А. В. Родин // Инжиниринг и технологии. – 2020. – Vol. 5(2). – С. 1–4. – DOI 10.21685/2587-7704-2020-5-2-2.