

NFC как замена для наличных и банковских карт, и не только

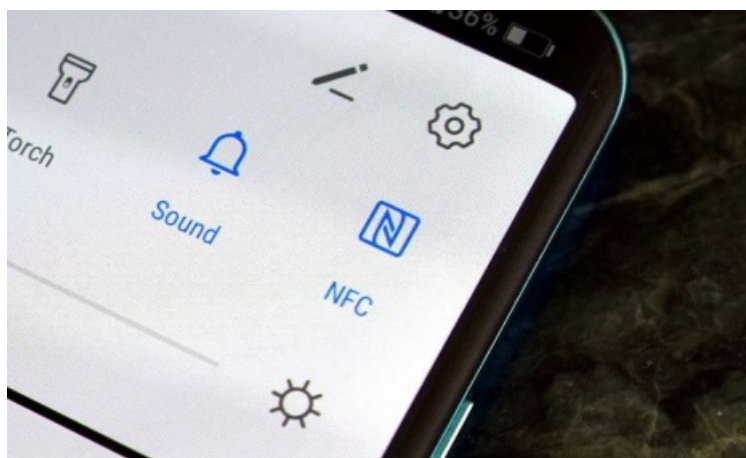
"OMNY призвана спасти нью-йоркцам их самый ценный товар – время", – заявлял Патрик Фойе, председатель MTA (Metropolitan Transportation Authority), на мероприятии, посвященном запуску системы бесконтактного платежа на станции метро Манхэттена в 2019 году. OMNY - One Metro New York, новая технология оплаты проезда, должна была внедряться поэтапно до 2023 года. Но пандемия коронавируса внесла свои коррективы, и власти города поспешили запустить систему, так как бесконтактный платеж исключает риск заражения вирусом через наличные и проездные или банковские карты. В Нью-Йорке, который лидирует по росту заболеваемости COVID-19 по всему США, OMNY почти полностью запущена к 1-января 2021 года.

С функцией Tap-to-Pay пассажиры для оплаты проезда в метро и автобусах могут пользоваться бесконтактными банковскими картами (кредитными или дебетовыми), а также смартфонами, подключенными к таким цифровым кошелькам, как Apple Pay, Samsung Pay или Google Pay, взамен пластиковых карт MetroCard, которые использовались с 90-х годов. Это должно снизить риск заражения коронавирусом, а также ускорить вход в автобус или станцию метро, и уменьшить расходы во всей транспортной системе. По сообщению MTA, сканеры OMNY установлены на 472 станциях метро и в 5 800 автобусных остановках.

[NFC как замена для наличных и банковских карт, и не только]

На данный момент для оплаты требуется смартфон, поддерживающий мобильные платежи на основе NFC, чтобы использовать систему OMNY. Позже, в 2021 году MTA начнет продавать карты с поддержкой tap-to-pay, которые можно будет использовать вместо смартфона - важное дополнение, поскольку не у всех пассажиров есть смартфон.

Но сегодня смартфон есть практически у всех. И почти все современные смартфоны выпускаются с поддержкой NFC (Near field communication) - технологии беспроводной передачи данных малого радиуса действия, которая даёт возможность обмена данными между устройствами. Эта технология - простое расширение стандарта бесконтактных карт (ISO 14443), которое объединяет интерфейс смарт-карты и считывателя в единое устройство и определяет использование свободного (нелицензируемого) диапазона частот 13,56 МГц с амплитудной модуляцией и девиацией 850 кГц. Дальность действия - 10 см. Скорость обмена - от 106 до 848 кбит/с.



NFC в смартфоне служит не самостоятельным средством передачи данных, а своего рода командным устройством. Обмен информацией осуществляется через беспроводное соединение. NFC дает команду на включение Bluetooth или Wi-Fi и передачу файла. Преимущество технологии в том, что связь между двумя устройствами устанавливается мгновенно. Теоретически возможен обмен любыми файлами, в том числе аудио и видео. Но из-за их большого объема скорость передачи окажется очень низкой. Поэтому обычно пользователи обмениваются не файлами, а ссылками на них. Скорость обмена данными у NFC она гораздо ниже, чем у Bluetooth. Поэтому для обмена файлами большого объема эта технология не подходит. Средством передачи аудио, видео, фото как раз служит Bluetooth (или другой модуль беспроводной связи - Wi-Fi), а NFC обеспечивает мгновенное соединение.

Модуль NFC присутствует во многих современных смартфонах, но не все имеют представление о том, зачем он нужен и как им пользоваться. Между тем эта функция очень удобна, и прежде всего для бесконтактной оплаты покупок.

Бесконтактные платежи - самая востребованная и актуальная область использования технологии NFC. Это удобно и быстро: для оплаты не требуется предоставлять карту кассиру и вводить PIN-код. Достаточно просто поднести смартфон к терминалу, и платежные данные будут переданы автоматически.



В NFC связь поддерживается посредством индукции магнитного поля, где две рамочные антенны располагаются в пределах ближнего поля друг друга, эффективно формируя трансформатор с воздушным сердечником. Благодаря компактным размерам и низкому потреблению энергии NFC можно использовать в небольших устройствах. В смартфонах антенна часто крепится на задней стороне гаджета, под крышкой. Чтобы у пользователей не возникало вопроса, как именно прикладывать гаджет для передачи данных (особенно такая проблема характерна для планшетов из-за их большого размера и маленького радиуса действия технологии), местонахождение чипа часто помечается специальной наклейкой на корпусе.



Технология NFC базируется на RFID (Radio Frequency IDentification) - методе автоматической идентификации объектов. Посредством радиосигналов считываются или записываются данные, хранящиеся в так называемых транспондерах, или RFID-метках. То есть это технология передачи информации по радиоканалу, которая поддерживает как активные, так и пассивные устройства. Метки NFC - это небольшие программируемые информационные зоны, которые можно встраивать в афиши, рекламные щиты или на полках с продукцией в розничных магазинах. "Коснувшись" метки, можно получить дополнительную информацию, например карты, веб-адреса и рекламные ролики фильмов.

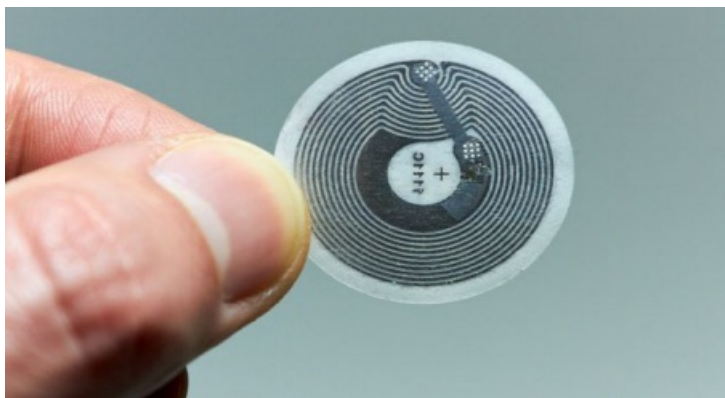
Самое главное преимущество NFC - это короткое время соединения, одна десятая секунды, а малый радиус действия делает этот способ передачи информации более защищенным.

NFC позволяет передавать данные со скоростью 424 Кбит/с, что гораздо меньше, чем у Bluetooth.

Развитие технологии бесконтактных платежей привело к появлению таких карт как Visa PayWave и MasterCard PayPass, имеющих встроенную антенну и работающих по стандарту NFC.

NFC может найти применение и в "умных домах". Метки можно интегрировать не только в платежные терминалы, турникеты метро, смарт-карты, а также в специальные аксессуары - брелоки, браслеты, бытовую технику и т.п. Это может быть удобным в быту и намного упростить рутинные дела.

Благодаря этой технологии вам не придется всякий раз изучать меню того или иного гаджета, чтобы найти в нем ту или иную функцию. Конечно, предварительно метку потребуется запрограммировать на нужное действие. Это делается просто с помощью специальных приложений, таких как NFC Task Launcher или NFC ReTag.



Ну и один из главных вопросов, волнующих пользователей в связи с бесконтактными платежами, - это безопасность. Каким образом обеспечивается защита передачи данных, например в Android Pay? Как и в других платежных системах, информация о карте и ее держателе не поступает на терминал. Для каждой оплаты в облаке формируется индивидуальный ключ - так называемый токен. Данные карты, необходимые для создания токенов, хранятся на сервере Google в зашифрованном виде. Таким образом, перехватить их в момент оплаты невозможно. Для защиты процесса транзакции в Android Pay используется сканирование отпечатка пальца, а также PIN-код, пароль, идентификация лица.

А могут ли злоумышленники отправить вредоносный файл или получить доступ и управление над NFC-устройством?

Да, могут. Но не все так просто.

На NFC-устройства можно сделать атаки с использованием ретрансляции (Relay attack). Для этого нападения злоумышленник должен отправить жертве запрос считывателя и её ответ в режиме реального времени передать дальше на считывающее устройство. Это делается для того, чтобы выполнить задачу, симулирующую владение смарт-картой жертвы.

Однако на практике такая атака довольно затруднительна в связи с жёсткими ограничениями по времени на ответ запрашиваемого устройства. В некоторых случаях речь может идти о микросекундных допусках, также ввиду маленького расстояния взаимодействия атаки с использованием ретрансляторов очень проблематичны.

Разрушение данных относительно легко осуществить средствами радиоэлектронной борьбы (РЭБ), то есть глушилками RFID. Нет способа предотвратить такое нападение, однако единственным его результатом будет невозможность установить связь. Несанкционированная модификация данных внутри сообщения атакующим устройством нереализуема на практике в связи с невозможностью предсказать амплитуду и сдвиг фазы наведённого сигнала на приёмном устройстве. RFID-приёмник чувствителен к внезапной смене амплитуды и фазы несущего сигнала.

Также, радиочастотный сигнал беспроводной передачи данных может быть перехвачен антеннами. Расстояние, с которого атакующий в состоянии подслушать радиочастотный сигнал, зависит от многочисленных параметров, но в любом случае - это всего несколько метров. Кроме того, на подслушивание чрезвычайно влияет режим связи. Устройство без собственного источника питания, которое производит очень слабый радиосигнал, намного тяжелее подслушать, чем устройство с источником питания. Стандарт NFC сам по себе не предлагает защиты против подслушивания, но стек протоколов использует криптоалгоритмы поверх NFC для защиты данных.

Нью-Йорк - это третий город, городской общественный транспорт которого полностью перешел на бесконтактную оплату. Первыми были Лондон и Сидней. А дальше - больше. Все крупные мировые города будут переходить на такую систему оплаты. И это касается не только сферы транспорта. NFC развивается и находит свое применение в следующем:

- электронная покупка билетов (авиабилеты, билеты на концерт, и другие); - скидочные, бонусные, подарочные и другие карты лояльности; - электронные деньги;
- карты путешественника;
- удостоверения личности;
- мобильная торговля;
- контроль качества (NFC-метки вместо штрих-кода, QR-кода); - медицина (отслеживание пациентов через NFC-браслеты, доступ к истории болезни и т.д.);
- электронные ключи - ключи от машины, ключи от дома/офиса, ключи, гостиничного номера, и т. д.;
- игровая индустрия;
- IoT;
- для конфигурирования и инициализации других беспроводных соединений, таких как Bluetooth,

Wi-Fi или Ultra-wideband.

