А. В. Стариковский, А. В. Зуйков, М. С. Аристов, Д. А. Степаньян

АТАКИ НА МОБИЛЬНЫЕ ТЕЛЕФОНЫ, ИСПОЛЬЗУЮЩИЕ УЯЗВИМОСТИ ТЕХНОЛОГИИ NFC

Мобильные технологии развиваются быстро, и модельный ряд телефонов обновляется чуть ли не каждый день. Но буквально несколько лет назад на рынке мобильных устройств появился аппарат нового поколения, который в ближайшие годы имеет все возможности перевернуть наше представление о столь привычном уже устройстве, — телефон с поддержкой NFC.

NFC (Near Field Communication) — технология беспроводной связи малого радиуса действия, которая позволяет производить обмен данными между устройствами, находящимися друг от друга на расстоянии около 10 сантиметров. Встроенный передатчик NFC позволяет существенно увеличить функциональность мобильного аппарата. Так, если поднести телефон на расстояние всего лишь 5—10 сантиметров к специальной метке, то информация, содержащаяся в такой метке, немедленно появится на экране устройства. Верно и обратное: информация с телефона может быть передана на считыватель бесконтактно. Такие телефоны уже применяются и приобрели большую популярность в Японии и Европе. На очереди Россия.

Применений революционной технологии NFC множество. Телефон можно использовать как кредитную карту или для оплаты проезда в метро. Все, что для этого необходимо, — поднести его к терминалу оплаты или турникету. К сожалению, стремительное развитие NFC-аппаратов приводит к тому, что уязвимые сами по себе мобильные телефоны получили дополнительно целый ряд серьезных недостатков, присущих новой технологии.

Устройство с NFC-модулем можно вывести из строя без ведома владельца. Причем сделать это крайне легко, лишив тем самым пользователя и наличных денег, и даже ключа в собственный офис или гостиничный номер [1].

Для того чтобы понять, почему NFC-телефоны могут быть так легко выведены из строя, проведем небольшой анализ данной технологии. Как уже было сказано, рассматриваемые аппараты имеют NFC-модуль, который позволяет им с небольшого расстояния считывать информацию со специальных меток. Метка состоит из элемента памяти и антенны, которая принимает излучаемый телефоном радиосигнал. Энергия радиосигнала используется для считывания данных из памяти и модуляции ответной радиоволны, которая и улавливается телефоном.

Обратимся теперь к реализации NFC-метки и особенностям NFC-телефона.

Данные, записываемые в метки, которые считывают NFC-аппараты, формируются согласно утвержденному формату NDEF (NFC Data Exchange Format), который позволяет хранить в одной метке записи различных типов. Сообщение NDEF начинается с флага MB (Message Begin), т. е. указания на «Начало данных». Последним полем должен быть флаг ME (Message End) — «Конец сообщения». Между ними находятся так называемые записи, каждая из которых служит для хранения данных соответствующих типов. Записи, помещенные в структуру, не зависят друг от друга, могут иметь произвольный размер и характеризуются следующими параметрами: типом, длиной и идентификатором.

Длина записи определяется в октетах (1 октет равен 8 битам). Параметр «Тип записи» указывает на хранимый тип данных. По этому значению приложение-обработчик, получающее NDEF-сообщение, может перенаправить полученную информацию непосредственно той программе, которая предназначена для ее обработки. Параметр «Идентификатор записи» является необязательным и предназначен для дополнительных атрибутов, которые помогут приложению обработать данные, хранимые в записи.

Записи в NDEF-структуре помещаются последовательно друг за другом и имеют сквозную нумерацию. Извлечением и передачей их соответствующим приложениям занимается специальная программа NFC-парсер. Она обращается к каждой записи, определяет ее длину и тип, после чего на основе этой информации вычисляет, сколько бит данных и какому приложению должно быть передано.

К сожалению, в погоне за лидерством на рынке компании-производители мобильных телефонов допустили ряд существенных ошибок в разработке встроенных парсеров NDEF-структур [2]. NFC-парсеры телефонов не выполняют проверку ошибок в формате NDEF-сообщений. Злоумышленники часто пользуются этим. Указание в параметре «Длина записи» числа 0xFFFFFFFF приведет к отключению считавшего метку мобильного устройства, так как в NFC-парсерах современных телефонов нет проверки факта переполнения и при обработке приведенного числа программа попытается выделить размер памяти для записи NDEF-структуры, который будет существенно превышать допустимый для телефона объем.

Используя рассмотренную уязвимость, злоумышленник может создать NFC-метки, которые при прикосновении телефона будут выводить последний из строя. Для того чтобы заставить пользователя прикоснуться к подобной метке, атакующий может прибегнуть к различным приемам. Мошенник может развесить красочные рекламные постеры, которые будут обещать абонентам мобильной связи бесплатно получить мелодию или обои для своего телефона, всего лишь прикоснувшись своим устройством к метке на плакате. Также злоумышленник может заменить настоящие информационные метки в музее на собственные «смертоносные» данные.

Защититься от подобного рода атак можно, соблюдая осторожность при выборе NFC-меток. Так как технология позволяет работать только в пределах 10 сантиметров, то у мошенников не так много шансов на успех.

В NFC-метке могут храниться данные любых известных типов. Самыми распространенными и популярными из них являются Smart Poster, URI, vCard.

Smart Poster — это формат данных, указывающих на ресурс, содержащий подробную информацию об идентифицируемом предмете. Этот тип становится все более популярным. Такие метки часто помещаются на рекламные плакаты в городах, на экспонаты в музеях, на объявления для того, чтобы заинтересовавшийся информацией обладатель мобильного телефона нового поколения мог быстро и беспрепятственно получить доступ к ресурсу, где приведены более подробные данные.

Smart Poster существенно отличается от формата URI, который представляет собой просто указание на информационный ресурс. Формат Smart Poster содержит помимо этого также последовательность действий, которые должен произвести телефон для того, чтобы пользователю немедленно были предоставлены интересующие его сведения. Например, Smart Poster подразумевает открытие web-браузера на нужной странице интернет-ресурса.

Рассмотрим подробнее, что происходит с мобильным устройством, когда пользователь подносит его к «умному плакату». Сначала NFC-передатчик получает сообщение, содержащее запись формата Smart Poster, с метки плаката и приступает к его анализу. Данный формат подразумевает наличие следующей структуры.

В поле URI хранится ссылка на ресурс, где находится необходимая пользователю информация. В поле Text содержится комментарий к открываемой ссылке. А в поле Action записана команда вызова приложения мобильного телефона, которое может открыть ссылку и верно интерпретировать ее (например, web-браузер).

Отметим, что поле Text в формате Smart Poster имеет специальное назначение. Именно основываясь на информации, передаваемой в нем, пользователь принимает решение о том, стоит ли

открывать полученную ссылку. Когда NFC-передатчик мобильного телефона считал сообщение, он отображает на экране содержимое поля Text и собственно ссылку, предлагая владельцу подтвердить или отклонить ее вызов. На этом праве выбора и построена защита телефона.

К сожалению, существует возможность ввести пользователя в заблуждение и заставить его открыть совсем не ту ссылку, которую он хотел бы прочитать.

Рассмотрим, как злоумышленник может это сделать. Для этого необходимо подменить NFC-метку на «умном плакате», а также сформировать такое ее содержимое, которое покажет пользователю ту же информацию, что предлагалась бы оригиналом, но при этом переадресует его на страницу с вирусом.

Для формирования собственной NFC-метки применяется специальное устройство NFC-Encoder, которое находится в свободной продаже, и пустая перезаписываемая метка, которую также можно легко приобрести. Для подмены информации можно использовать ошибку, которую допустили создатели NDEF-стандарта сообщений. Мобильный телефон с NFC-передатчиком может отобразить на экране лишь фиксированное количество строк, которые записаны на NFC-метке [3]. Когда количество строк превышает некоторую возможную величину, информация просто перестает отображаться. Это верно и для сообщения, появляющегося на экране телефона при запросе подтверждения перехода на ресурс в сети Интернет.

Рассмотрим, как подобной ситуацией пользуется злоумышленник. Предположим, объектом атаки является пользователь, который хочет обратиться к информационному плакату агентства по прокату автомобилей за границей. При поднесении телефона к обыкновенному плакату на экране отображается следующее сообщение:

Прокат автомобилей во Франции
http://www.auto-in-france.ru

Первая строка сообщения хранится в формате Smart Poster в поле Text, а вторая — в поле URI.

А теперь приведем сообщение, которое злоумышленник может поместить в свою собственную NFC-метку:

Прокат автомобилей во Франции\rhttp://www.auto-in-france.ru\r\r\r
http://www.virus2.ru

Символ \r означает перенос каретки, т. е. переход на новую строчку. При интерпретации данных на экране телефона приведенное сообщение будет выглядеть ровно так же, как эталонное. Строка поля URI на экране телефона не появится, так как количество строк, которые он может отобразить, будет превышено. В случае подтверждения перехода пользователь попадет на страницу http://www.virus2.ru, с которой он немедленно получит вирус на свой телефон.

Защититься от атаки можно, ведь большинство браузеров мобильных телефонов отображают адрес открываемой страницы. Так как скорость мобильного Интернета, как правило, достаточно мала, то переход на страницу злоумышленника можно прервать, вовремя заметив подмену.

В столицах стран Европы и в Японии мобильные телефоны используются для оплаты поездок на метро. Этот вид сервиса прост и удобен. Покупать билет на метро теперь нет никакой необходимости — достаточно подойти к специальному постеру рядом с кассой и поднести к нему телефон. На экране мобильного устройства появится следующий текст: «Для оплаты проезда подтвердите покупку билета, отправив SMS на указанный короткий номер». После этого обладателю мобильного аппарата необходимо подтвердить покупку билета отправкой указанного SMS-сообщения, и, приложив телефон к турникету метро, он сможет пройти дальше. Но, к сожалению, данная возможность может позволить злоумышленнику снять все деньги со счета пользователя без его ведома. А виной этому — уязвимости новой технологии.

Данная атака очень похожа на рассмотренный выше вариант, но имеет ряд особенностей, на которых остановимся подробнее.

Атака основана на подмене злоумышленником NFC-метки с целью перенаправления перевода денег пользователя не на счет метрополитена, а в «карман» мошенников. Для этого нет необходимости применять методы, описанные выше. При вызове некоторого адреса в сети Интернет пользователь, увидев саму ссылку, мог заподозрить наличие угрозы. В рассматриваемом же случае вряд ли неизвестный телефонный номер может что-то сказать пользователю. Для достижения своих целей злоумышленник планирует следующие действия. Во-первых, ему необходимо выкупить короткий номер у оператора. Подобные номера позволяют брать деньги с пользователей мобильных телефонов в случае, если на него производится звонок. Напомним, что по законам многих стран деньги с мобильного счета пользователя может взимать лишь сотовый оператор, SIM-картой которого пользуется абонент. Именно поэтому для хищения средств со счета мошенники применяют так называемые короткие номера. К финансовым средствам, вырученным от их использования, злоумышленник может получить доступ после того, как уплатит оговоренный процент от выручки оператору. Также атакующим необходимо изготовить метки и корректно записать информацию в них. Как уже говорилось ранее, средства и устройства для достижения данных целей находятся в свободной продаже. В метку обычно заносятся следующие данные:

Для приобретения билета необходимо сделать вызов по следующему телефонному номеру +923423423.

При прикосновении телефона к NFC-метке эта информация появляется на экране. Далее пользователь может нажать кнопку «Подтвердить» либо «Отклонить». В первом случае будет сделан вызов на указанный номер. Если пользователь «попал» на ложную NFC-метку, то он лишится определенной суммы со своего счета.

Для того чтобы ваши деньги не перешли злоумышленнику, необходимо воздержаться от использования NFC-телефонов для оплаты покупок, так как эта система по-прежнему несовершенна.

Также стоит отметить тот факт, что злоумышленника, использующего приведенный алгоритм, достаточно просто обнаружить и привлечь к ответственности. Сотовые операторы почти всегда располагают данными о тех, кто выкупает короткие номера с целью получения прибыли.

Рассмотрим атаки на системы, которые используют для оплаты короткие SMS-номера. Подобные сотовые номера аналогичны используемым при проведении предыдущей атаки с той разницей, что они принимают SMS-сообщения. Обычно цена одного такого сообщения сопоставима с ценой газеты или журнала.

Еще одной особенностью атаки является то, что, реализуя ее, злоумышленник рискует гораздо меньше, чем в предыдущем случае. Аренда короткого номера не требуется. Все, что нужно атакующему, — найти два уличных киоска, где продаются товары с использованием автоматизированной системы продаж (т. е. без участия оператора), поддерживающей NFC-технологию. После этого необходимо скопировать содержимое NFC-метки с первого киоска и поместить поддельную клонированную метку на место штатной метки на втором. Таким образом, получается, что атакуемый, купив с помощью мобильного телефона товар во втором киоске, сам того не подозревая, оплачивает, например, газету из первого. Злоумышленнику остается лишь ожидать, когда первый киоск совершенно безвозмездно выдаст газету или журнал. А вот пострадавший не сможет получить ничего.

Защититься от подобной атаки не удастся. Даже бдительность не поможет избежать обмана. Так что прежде чем воспользоваться подобного рода оплачиваемыми услугами, стоит взвесить все «за» и «против».

Рассмотренные выше разновидности атак на мобильные устройства, оснащенные NFC-передатчиками, позволяют утверждать, что эта технология обладает большим количеством уязвимостей и требует доработки в сфере обеспечения безопасности пользователей. Для предотвращения утечки личных данных и средств с абонентских счетов можно рекомендовать отказаться от использования NFC-технологии для оплаты товаров и услуг, а также сохранять бдительность в остальных случаях.

СПИСОК ЛИТЕРАТУРЫ:

1. *Михайлов Д. М., Стариковский А. В.* Исследование механизмов проведения атак на RFID-системы // Материалы II Всероссийской научной конференции «Научное творчество XXI века». Красноярск: Научно-инновационный центр, 2010. С. 16–17.
2. *Haselsteiner E., Breitfuss K.* Security in near field communication (NFC) // Philips Semiconductors. Printed handout of Workshop on RFID Security. RFIDSec. July 2006. P. 51–53.
3. *Roland, Langer, Scharinger.* Security Vulnerabilities of the NDEF Signature Record Type // 3rd International Workshop on Near Field Communication (NFC). 2011. P. 34–35.