УДК: 004.056

# УГРОЗЫ И СПОСОБЫ ЗАЩИТЫ RFID И NFC МЕТОК

**Ковынёв Н.В.**
*Московский государственный технический университет имени Н.Э. Баумана*
*Москва, Российская Федерация*

В настоящее время метками на основе ближней радиосвязи (NFC) и радиочастотными метками (RFID) оснащаются многие товары повседневного пользования, включая кредитные и платежные карты, водительские удостоверения, идентификационные карты, паспорта, проездные билеты на метро и т.д. NFC и RFID чипы, использующие беспроводную радиосвязь для передачи информации, также находят применение в аптеках для отслеживания, транспортировки и отправки продукции.

Эти технологии позволяют пользователям активировать карточки с помощью сканирования, не прикасаясь к терминалу, так как RFID и NFC срабатывают даже в бесконтактном режиме. Однако технологии RFID и NFC имеют ряд уязвимых мест, которые при отсутствии необходимых мер безопасности облегчают мошенникам кражу ценной информации. Сразу после появления NFC и RFID на рынке в их работе были выявлены неожиданные просчеты, поэтому существуют определенные опасения в отношении возможности считывания и копирования информации с таких карт хакерами.

Электронные кражи (e-pickpocketing) – это новый термин для обозначения кражи информации с карты без какого-либо контакта с ней. Чипы RFID позволяют считывать данные на расстоянии до нескольких метров. Все, что нужно для связи с меткой в документах – купить готовое устройство на eBay.Считыватели близкого радиуса действия стоят около 50 долларов, дальнего – порядка сотни. После считывания у злоумышленника на руках остается полная электронная копия всей информации RFID-метки. С ее помощью можно сделать поддельную копию, либо использовать другими методами – в зависимости от типа украденного документа.Терминалы будут воспринимать копию в качестве оригинала. Доказать обратное практически невозможно [1].

Рисунок 1 – Пример считывания RFID

NFC фактически является вариацией RFID, хотя и обладает меньшей дальностью – всего несколько сантиметров. Но это – только для заводских, лицензионных устройств.Исследователи из британского Университета Суррей смогли считать данные по NFC на расстоянии до 80 см. Испанские хакеры и вовсе научили Android-смартфоны превращаться в ретранслятор NFC-сигнала, распространяющего собственные важные данные.Подобный подход позволяет провести платеж прямо через смартфон владельца. Но есть и другие способы.Например, подключившись через NFC другим смартфоном или серийно выпускаемым ридером с помощью приложения все необходимые данные карт, использованных при операциях в браузере. Далее достаточно найти магазин, позволяющий проводить оплату без ввода указания CSV-кода (а такие еще существуют). Учитывая серьезность проблемы электронных краж, ученые предлагают новые технологии обеспечения безопасности RFID-карт. Давайте рассмотрим некоторые из этих инновационных методов.[2]


Рисунок 2 – Пример взаимодействия NFC

Если Вы предпочитаете изготавливать оборудование в домашних условиях (по принципу «Сделай сам»), Вы можете использовать два материала, препятствующие прохождению радиосигналов - воду и металл. Теоретически вода эффективно блокирует радиосигналы, однако такое решение довольно сложно воплотить в реальности. Металл намного более практичен в использовании, так как, например, алюминиевую фольгу можно приобрести везде, и она доступна по цене. Куска алюминиевой фольги толщиной минимум 27 микрон достаточно для блокирования сигналов RFID и NFC. Для защиты карты от считывания просто заверните ее в алюминиевую фольгу. Разворачивайте карту только перед использованием. Возможно, Вы будете иметь довольно странный вид, используя этот метод, но, тем не менее, он достаточно эффективен.

Вы можете выбрать более стильный вариант защиты и приобрести готовые защитные корпусы и бумажники, блокирующие RFID-сигналы. Такие компании, как, например, Identity Stronghold продают различные аксессуары, которые могут защитить карты от электронных краж. В настоящее время правительство США требует, чтобы все государственные служащие пользовались подобными защитными корпусами для идентификационных карт.

Репозиторий БГТУ

Для предотвращения копирования меток RFID и NFC можно использовать криптографию. Одноразовый код или код, непрерывно изменяющийся после каждого сканирования, можно использовать для того, чтобы помешать перехватчикам записывать операции для последующего воспроизведения. Даже если мошенникам удастся украсть одноразовый код, они не смогут им воспользоваться.

Для более сложных устройств также можно использовать аутентификацию методом «запрос-ответ» в тех случаях, когда метка взаимодействует с ридером. При таком типе аутентификации ридер выдает метке запрос, а метка в свою очередь отвечает секретным цифровым кодом, который может быть основан на симметричной или двухключевой криптографии. При использовании этого протокола, информация не передается по небезопасному каналу связи между ридером и меткой.

Ученые Инженерной школы Свенсона Питтсбургского университета (Pittsburgh Swanson School of Engineering) разработали метод предотвращения мошенничества с RFID с помощью использования технологии включения и выключения карты при контакте с ее определенным участком при сканировании.

Профессор Марлин Микл (Marlin Mickle), доктор технических наук и исполнительный директор Научно-инновационного центра по RFID-технологиями (RFID Center for Excellence) в Школе Свенсона заявил, что новая технология «позволяет блокировать кредитные карты на основе RFID или NFC, когда они лежат в кармане или на столе, и предотвращает их считывание мошенниками с использованием портативных сканеров». Карту невозможно считать, пока кто-либо не включит ее.

«Наша новая разработка включает антенну и электросхему, контакты которой можно разомкнуть простым переключением, как, например, при выключении освещения дома или в офисе, - говорит Микл. - Кредитная карта на основе RFID или NFC блокируется, если она остается в кармане или лежит на какой-либо поверхности, и мошенники не могут считать ее с помощью портативных сканеров. Это весьма простое и недорогое решение, которое можно использовать в процессе изготовления кредитных карт на основе RFID и NFC. Мы подали заявку на патент и надеемся на скорое внедрение этой технологии после одобрения патента» [3].

Впрочем, стоит помнить, что металлический кошелек или визитница для карт не исключают возможность кражи данных карт.

1. Не включайте NFC без надобности, не держите его постоянно включенным.

2. То же касается других беспроводных интерфейсов – Bluetooth и Wi-Fi.

3. Проверяйте активность фоновых процессов, при частом обращении к сетевым интерфейсам неподходящих для этого приложений – проверьте смартфон антивирусом.

4. Не устанавливайте приложения из непроверенных источников.

5. Не теряйте и не оставляйте смартфон в людных местах – как средство доступа к данным он может принести куда большую выгоду, вернувшись в ваши руки.

1. Михайлов Д.М., Стариковский А.В. Исследование механизмов проведения атак на RFID-системы// Материалы 2 Всероссийской научной конференции «Научное творчество 21 века». Красноярск: Научно-инновационный цетр, 2010. – С. 16–17.
2. Стариковский А.В., Зуйков А.В., Аристов М.С., Степаньян Д.А. Ататки на мобильные телефоны, использующие технологии NFC//Безопасность информационных технологий. – 2012. – №2. – С. 60–64.
3. Макаров В.В., Мамонов С.К. Применение NFC-технологий в мобильных платежах// В мире науки и инноваций: сборник статей по материалам международной научно-практической конференции: в 2 ч. – 2017. – С. 17–21.

*УДК 681*

## ТЕХНИЧЕСКИЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ РАДИАЦИОННОЙ БЕЗОПАСНОСТИ НА СТЕРЕОТАКСИЧЕСКОМ ЛИНЕЙНОМ УСКОРИТЕЛЕ ЭЛЕКТРОНОВ TRUEBEAM STX В ГУ «РЕСПУБЛИКАНСКИЙ НАУЧНО-ПРАКТИЧЕСКИЙ ЦЕНТР ОНКОЛОГИИ И МЕДИЦИНСКОЙ РАДИОЛОГИИ ИМ. Н.Н. АЛЕКСАНДРОВА»

**Петкевич М.Н. [1], Титович Е.В.[1], Герцик О.А.[1], Потепалов П.О.[1], Киселев М.Г.[2]**
*[1]РНПЦ онкологии и медицинской радиологии имени Н.Н. Александрова*
*[2]Белорусский национальный технический университет*
*Минск, Республика Беларусь*

**Цель работы:** Основным источником радиационной опасности при работе медицинского линейного ускорителя является генерируемое им тормозное излучение широкого энергетического спектра. В дополнение к тормозному излучению при энергии фотонов выше порога реакции (≥10 МэВ) происходит фотоядерная реакция и образуются вторичные нейтроны. Для обеспечения радиационной безопасности как персонала, так и пациентов, ускоритель должен быть оснащен системой радиационного контроля, которая использует дозиметрические приборы,

Репозиторий БНТУ