Эссе по курсу "Защита информации", кафедра радиотехники,
Московский физико-технический институт (ГУ МФТИ),
http://wwwremiptru/infsec

Бесконтактные смарт-карты
(Contactless smartcards)

Косарев Николай Евгеньевич, 312 гр
24 апреля 2007 года

1. Введение

Эта статья посвящена бесконтактным смарт-картам, а именно, что наиболее интересно на мой взгляд, банковским дебетовым и кредитным пластиковым картам, а также их безопасности и перспективам. Начнем издалека.

Бесконтактная смарт-карта (contactless smartcard) – смарт-карта, которая может обмениваться информацией с другими устройствами без прямого физического контакта с ними, используя технологию радиочастотной идентификации (**RFID** technology, **R**adio-**F**requency **ID**entifier technology). Эта технология основана на специальных устройствах, называемых RFID тегами (RFID tags), которые находятся внутри объекта (в данном случае карты) или прикрепляются к нему (см. рис. 1). Они обязательно содержат кремниевый чип и антенну, для излучения радиоволн. Различают активные и пассивные теги. Их отличие в том, что активные теги требуют постоянного источника питания, в то время как пассивные получают необходимую энергию из радиочастотного сигнала. Очевидно, что именно пассивные теги применяются при изготовлении бесконтактных смарт-карт. Стоит заметить, что бесконтактные смарт-карты становятся популярными в таких приложениях, как карты идентификации, электронные паспорта и др. Такие устройства, как правило, изготавливаются для работы с короткого расстояния (~10 см), но существуют RFID карты, которые способны работать на удалении в полметра и больше.

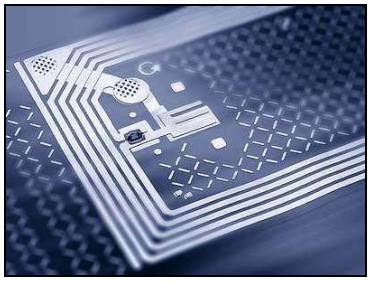

Рис.1. RFID тег.

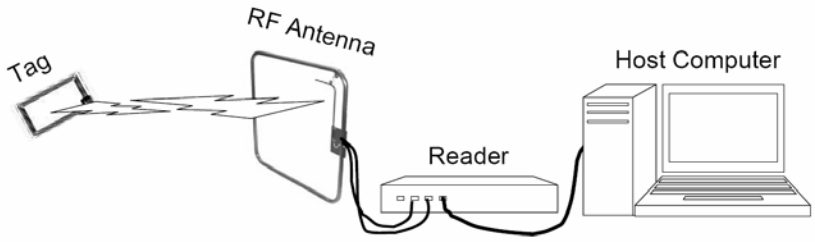

Рис.2. Принцип использования RFID смарт-карт.

2. Преимущества бесконтактных смарт-карт

Рассмотрим основные преимущества бесконтактных смарт-карт. Прежде всего, потребители получают возможность выбрать между традиционными картами с магнитной полосой и бесконтактными устройствами. В случае использования бесконтактных карт не нужно беспокоиться о том, где и как вставлять карту, как быстро проводить карту через считывающее устройство **POS** (**P**oint **O**f **S**ale)-терминала. Их можно использовать там, где транзакции должны происходить максимально быстро, без использования рук и вытаскивания карты из бумажника. Бесконтактные смарт-карты могут содержать в несколько раз больше информации, чем традиционные карты с магнитной полосой. Они также обрабатывают данные и выполняют различные вычислительные операции. Заметим, что вся эта функциональность реализуется без необходимости в активном источнике питания. Бесконтактные смарт-карты не требуют особого аккуратного ношения, так как они не содержат активных частей на поверхности и отдельных участков контакта со считывающими устройствами.
Конечно, RFID карты неидеальны. Да, их можно согнуть, сломать и вывести из строя механическим путем. Но одним из главных недостатков для потребителей, возможно, является их уязвимость к атакам злоумышленников.

3. Атаки

Сообщество по безопасности RFID устройств выделяет несколько атак на бесконтактные кредитные карты, отличающихся по сложности. Рассмотрим типовые.

3.1. Clandestine scanning / Тайное сканирование

В атаке тайным сканированием неавторизованное и потенциально скрытое считывающее устройство сканирует теги пластиковой карты с расстояния или в непосредственной близости от неё. Так как непрозрачные упаковки не обязательно непроницаемы для радиочастот, меры безопасности, достаточные для традиционных пластиковых карт, такие как «безопасные конверты» должны быть пересмотрены с учетом RFID технологии. Атака происходит, когда злоумышленник использует доступ к физическому потоку писем для чтения радиочастотных данных с кредитных карт во время передачи корреспонденции законным владельцам. Данная атака особенно опасна, так как атакующий получает дополнительную информацию (адрес владельца карты), используя, например, адресные книги, а также, так как физический доступ к почтовым отправлениям довольно прост (почтовые ящики на домах, либо расположенные у дороги).
Существует множество других подобного рода атак, таких как сканирование содержимого бумажника в толпе людей на эскалаторе или в метро.

3.2. Replay and relay attacks / Атаки повтора и замены

В атаке повтора (*replay attack*), злоумышленник передает точный радиочастотный ответ, записанный с прошедшей транзакции между считывающим устройством и бесконтактной картой Хотя существуют способы для предотвращения простых воспроизве-

дений информации (такие как временной штамп, единовременные пароли и криптография оклика и отзыва), но зачастую может успешно применяться более изощренная атака. Такая атака, известная как атака путем замены (*relay attack*), используется злоумышленником для подмены соединения от авторизованного считывающего аппарата через один или несколько иных устройств к легальной карте, которая может быть на значительном расстоянии. Расстояние, с которого атака заменой может успешно применяться, ограничено только задержкой, допустимой протоколом передачи.

3.3. Cross contamination attack

Cross contamination attack (атака перекрестного "заражения") происходит, когда личная информация, то есть имя владельца карты, номер, срок действия карты, становится известной злоумышленнику в радиочастотном контексте и затем используется в ином контексте. Например, злоумышленник мог бы использовать полученные данные для создания карты с магнитной полосой, перекодировать магнитную полосу на существующей карте или использовать данные для совершения транзакций без непосредственного применения карты, таких как онлайн покупки не требующих **CVC** (**C**ard **V**erification **C**ode) или заказ по телефону

4. Анализ атак

Если использовать типовое считывающее устройство для отправки запросов на бесконтактные пластиковые карты, то можно выделить четыре группы последовательных данных (для карт эмитентов A, B, C или D), получаемых радиочастотной аппаратурой в ответ на запрос. Анализируя эту информацию, можно выяснить, каким методам взлома потенциально подвержен каждый тип RFID карт.
Ниже приводятся результаты таких запросов и комментарии к ним. На каждом рисунке (рис. 3-6) информация поделена на 2 строки. Первая строка – ответ, полученный при считывании с магнитной полосы (приводится для сравнения), вторая строка – ответ полученный при считывании радиочастотным способом.

```
Bxxxxxx6531xxxxxx^DOE/JANE^09061010000000000000000000000000858000000
xxxxxx6531xxxxxx=09061010000085800000
```

Рис. 3. Данные, полученные от коммерческого считывающего устройства после радиочастотной транзакции с картой эмитента A

В полученном ответе, изображенном на рис.3, можно выделить номер счета, имя владельца, срок действия карты (в данном случае 06/2009) и некоторое статическое цифровое поле, не меняющееся от одной транзакции к другой.

Bxxxxxx1079xxxxxx^DOE/JANE^09011011000000000000100000000000
xxxxxx1079xxxxxx=09011011000*016*00221
Bxxxxxx1079xxxxxx^DOE/JANE^09011011000000000000100000000000
xxxxxx1079xxxxxx=09011011000*074*00231

Рис. 4. Данные, полученные от коммерческого считывающего устройства после радиочастотной транзакции с картой эмитента B Здесь мы видим дополнительный трехзначный код (выделенный жирным курсивом) и четырехзначный счетчик (выделен подчеркнутым шрифтом).

На рис.4 можно заметить четырехзначный счетчик транзакций и трехзначный код, который изменяется при каждом совершении транзакции. Эти три цифры, вероятно, являются результатом криптографического алгоритма, принимающего на вход счетчик транзакций и некоторый ключ, уникальный для каждой карты.

Bxxxxxx2892xxxxxx^DOE/JANE 017^1001101*10691958*
xxxxxx2892xxxxxx=1001101*10691958*01700
Bxxxxxx2892xxxxxx^DOE/JANE 018^1001101*40146036*
xxxxxx2892xxxxxx=1001101*40146036*01800

Рис. 5. Данные, после радиочастотной транзакции с картой эмитента C, отличаются от карты эмитента B Коды транзакции выделены жирным курсивным шрифтом, счетчик транзакций выделен подчеркнутым шрифтом.

Ответ карт типа C отличается от карт типа D в нескольких деталях, а именно он содержит восьмизначный уникальный код транзакции вместо трехзначного, счетчик транзакций находится в поле для имени владельца карты и имеет три знака вместо четырех. Стоит заметить, что вместо прямой отправки номера карты используется некоторый псевдоним.

Card #1:
77 0F 9F 61 02 *51 A0* 9F 60 02 *35 90* 9F 36 02 04 19 90 00
77 0F 9F 61 02 *C3 AF* 9F 60 02 *1D 5C* 9F 36 02 04 1A 90 00
Card #2:
77 0F 9F 61 02 00 0A 9F 60 02 00 64 9F 36 02 00 06 90 00
77 0F 9F 61 02 00 0A 9F 60 02 00 64 9F 36 02 00 07 90 00

Рис. 6 Эти линии представляют собой две пары байтовых строк от одного и того же запроса в последовательных радиочастотных транзакциях с двумя разными картами D B обоих примерах увеличивается 16 битный счетчик (показан подчеркнутым шрифтом). Для одной карты все остальные байты идентичны, а для другой можно заметить 32 битный код, поделенный на 16 битовые слова (показаны жирным курсивным шрифтом).

На рис.6 изображен ответ карт типа D. Дополнительный 32-битный код свидетельствует о наличии определенного механизма защиты, но, по крайней мере, некоторые типы коммерческих считывающих устройств не используют его и не передают в обрабатывающую платежи сеть.

Исходя из полученных данных, можно выделить несколько подходов для применения атак. Начнем с атаки повтором (*replay attack*):

1. *Неограниченный повтор*: Карты A и D, которые содержат статический ответ на запрос, сканируются один раз, после чего злоумышленник повторяет записанные данные. Обрабатывающая сеть не может зафиксировать отличия между повтором и транзакцией с реальной картой.
2. *Повтор с опережением*: Карты со счетчиком и криптографическим кодом обладают большей защитой, если обрабатывающая операции сеть хранит и проверяет значения счетчика. Таким образом, если транзакция n была принята сетью, транзакции с номером меньшим либо равным, чем n будут отклонены. Однако даже если счетчики и коды карт B и C защищены криптографическим алгоритмом, злоумышленник может выдать карте запрос на транзакцию, а затем передать ответ в сеть раньше, чем у легального владельца будет шанс использовать карту. Тогда обрабатывающая сеть примет транзакцию злоумышленника и отклонит легальную.
3. *Перебор счетчика*: Если счетчик транзакций является единственным источником для получения криптографического кода, тогда количество кодов ограничено максимальным значением счетчика транзакций. В этом случае, злоумышленник, который обладает достаточным количеством времени вблизи карты, может построить базу данных всех возможных вариантов счетчика и соответствующих кодов, и, следовательно, имитировать поведение реальной карты. Карты B подвержены такому способу атаки

Атака заменой (*relay attack*): Даже в случае гипотетической карты, которая комбинирует счетчик транзакции с протоколом, зависящим от запроса, атака заменой все еще может применяться. Например, если злоумышленник M_1 обладает скрытым считывающим устройством, которое соединено на радиочастоте с эмулятором карт зло-

умышленника M_2. M_1 может сидеть рядом или стоять с легальным владельцем A и устанавливать соединение с его картой, а M_2 одновременно использовать свой эмулятор на POS терминале. Таким образом, транзакция будет успешной, и сумма будет списана с владельца A.

Cross-contamination attack: Применяющиеся в настоящее время непрозрачные конверты, используемые для доставки банковской корреспонденции владельцу карты, не создают помех для считывания информации. Комбинируя полученные данные (номер карты, срок действия и имя владельца) с адресом доставки (уже известен, если корреспонденция была найдена в почтовом ящике, либо легко находится в адресной книге по имени владельца), легко совершить онлайн покупки не требующие CVC по картам типа A, B или D. Применение карт типа C затруднительно, т.к. в данном случае RFID считывающее устройство получает не реальный номер карты, а некоторый его аналог.

5. Меры противодействия. Заключение.

Для борьбы с незаконным применением бесконтактных карт можно использовать следующие дополнительные меры противодействия.
Например, «клетка Фарадея» - непрозрачная для некоторых радиочастот упаковка, которая предотвращает нежелательное сканирование карт. Ее можно применять для изготовления конвертов для доставки корреспонденции или специальных бумажников для ношения бесконтактных пластиковых карт.
Другой подход, несколько сложнее предыдущего, заключается в том, чтобы нарушить и запутать произвольное сканирование карты. Для этого применяют так называемый блокировочный тег (blocker tag), который имитирует наличие огромного количества несуществующих RFID устройств. Такой электронный прибор нужно хранить рядом с картой (например, в том же бумажнике) и при необходимости отключать нажатием на соответствующую кнопку при совершении покупки.
Новейший подход заключается в улучшении криптографических алгоритмов, используемых в бесконтактных смарт-картах. Если персональные идентификационные данные могут быть расшифрованы только соответствующим считывающим устройством, тогда использовать большинство из описанных выше атак проблематично. В настоящее время в некоторых странах Европы используется EMV (**E**uropay **M**astercard **V**isa) стандарт для взаимодействия кредитных карт и POS-терминалов. В этом стандарте для шифрования персональных данных применяются алгоритмы DES, Triple-DES, RSA или SHA Зашифрованная таким образом информация передаются центру обработки транзакций, на что, безусловно, тратится время и требуется наличие весьма значительных дополнительных вычислительных ресурсов у бесконтактной карты. Также существуют карты, основанные на криптографической технике DDA (**D**ynamic **D**ata **A**uthentication), при использовании которой карта подписывает случайные данные, полученные от считывающего устройства. Эта техника была разработана главным образом для терминалов, не имеющих подключения к обрабатывающей сети. Однако все эти криптографические усложнения бесконтактных карт увеличивают их стоимость в разы и требуют единого стандарта на изготовление карт и соответствующих POS-терминалов оплаты. Вероятно, по этой причине многие платежные ассоциации в настоящее время

вообще не используют алгоритмы симметричного шифрования или шифрования с открытым ключом, либо используют их в самом простейшем варианте.

6. Использованная литература

1. Thomas S. Heydt-Benjamin, Daniel V. Bailey, Kevin Fu, Ari Juels, Tom O'Hare: Vulnerabilities in First-Generation RFID-enabled Credit Cards, Oct. 2006.
2. Wikipedia materials:
   EMV - http://en.wikipedia.org/wiki/EMV
   Radiofrequency identification - http://en.wikipedia.org/wiki/RFID
   Smartcards - http://en.wikipedia.org/wiki/Smartcards
3. Ziv Kfir, Avishai Wool: Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems. School of Electrical Engineering, Tel Aviv University, Ramat Aviv 69978, Israel, 2005.