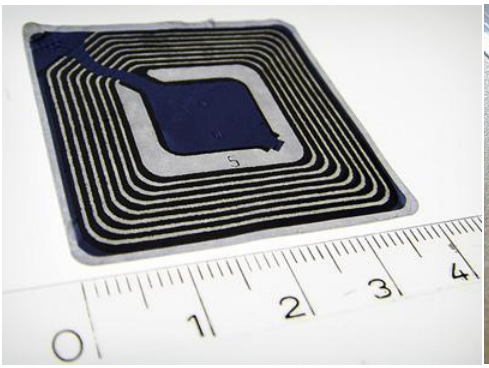
ЛЕКЦИЯ 5. УЯЗВИМОСТИ NFC, BLUETOOTH, ИК-ПОРТА, ETOKEN, ЧИПОВ И RFID-МЕТОК

5.1. УЯЗВИМОСТИ NFC

Near field communication, NFC («коммуникация ближнего поля», «ближняя бесконтактная связь») — технология беспроводной передачи данных малого радиуса действия, которая дает возможность обмена данными между устройствами, находящимися на расстоянии около 10 сантиметров, анонсирована в 2004 г.



Эта технология — простое расширение стандарта бесконтактных карт (ISO 14443), которое объединяет интерфейс смарт-карты и считывателя в единое устройство. Устройство NFC может поддерживать связь и с существующими смарт-картами, и со считывателями стандарта ISO 14443, и с другими устройствами NFC и, таким образом, — совместимо с существующей инфраструктурой бесконтактных карт, уже использующейся в общественном транспорте и платежных системах. NFC нацелена прежде всего на использование в цифровых мобильных устройствах.

Основные спецификации:

- Так же, как и в стандарте ISO 14443, 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. Этот стандарт работает в пределах общественно доступных и нелицензируемых радиочастот ISM band — Промышленные, Научные и Медицинские радиочастоты около 13,56 МГц, с шириной полосы пропускания почти 2 МГц;
- Рабочее расстояние с компактными стандартными антеннами: до 20 см;
- Поддерживаемая скорость передачи данных: 106, 212, или 424 кбод.
- Существуют два режима:
    - Пассивный режим связи: устройство Инициатор обеспечивает несущее поле, а целевое устройство отвечает посредством модулирования имеющегося поля. В этом режиме Целевое устройство может вытягивать свою рабочую мощность из предоставленной Инициатором электромагнитной области, таким образом делая Целевое устройство ретранслятором.
    - Активный режим связи: и Инициатор, и Целевое устройство взаимодействуют путём поочередного создания своих собственных полей. Устройство дезактивирует своё радиочастотное поле в то время, как оно ожидает данных. В этом режиме у обоих устройств должно быть электропитание.
- Для передачи данных NFC использует два различных вида кодирования. Если активное устройство передает данные со скоростью 106 кбод, тогда используется

модифицированный код Миллера со 100 % модуляцией. Во всех других случаях используется манчестерское кодирование с коэффициентом модуляции 10 %.

- Устройства NFC в состоянии одновременно и получать, и передавать данные. Таким образом, они могут контролировать радиочастотное поле и обнаруживать противоречия, если полученный сигнал не соответствует переданному.

Благодаря компактным размерам и низкому потреблению энергии NFC можно использовать в небольших устройствах. В смартфонах антенна часто крепится на задней стороне гаджета, под крышкой.

Области применения NFC:

- эмуляция карт: устройство NFC ведет себя как существующая бесконтактная карта;
- режим считывания: устройство NFC является активным и считывает пассивную RFID-метку, например для интерактивной рекламы;
- режим P2P: два устройства NFC вместе связываются и обмениваются информацией.
- мобильная покупка в общественном транспорте — расширение существующей бесконтактной инфраструктуры.
- мобильные платежи — устройство действует как платёжная карта.
- электронная доска — мобильный телефон используется для чтения RFID-меток, с уличных досок для объявлений, чтобы на ходу получать информацию.
- спаривание Bluetooth — для соединения устройств Bluetooth 2.1 и выше, поддерживающих NFC, достаточно сблизить их и принять соединение. Процессы поиска устройства и авторизации заменёны простым «прикосновением» мобильных телефонов.

5.1.1 Аспекты безопасности NFC

Атака с использованием эксплойта

На конференции EuSecWest по вопросам безопасности, прошедшей 19—20 сентября 2012 года, компанией MWR Labs был представлен эксплойт 0day, показавший уязвимость технологии NFC в мобильных устройствах. Специалистам по безопасности удалось передать через NFC-соединение вредоносный файл и получить полный контроль над принимающим устройством. Таким образом, конфиденциальные данные и денежные средства «жертвы» оказались под угрозой. Для предотвращения захвата контроля необходимо внесение доработок разработчиками устройств с целью ограничения активности данных, принятых посредством NFC.

Хотя радиус связи NFC ограничен несколькими сантиметрами, NFC сама по себе не гарантирует безопасности соединений. В 2006, Ernst Haselsteiner и Klemens Breitfuß описали различные возможные типы атак

Подслушивание

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. По идее, стек протоколов должен использовать криптоалгоритмы поверх NFC для защиты данных.

Модификация данных

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 наведенного сигнала на приемном устройстве. RFID-приемник чувствителен к внезапной смене амплитуды и фазы несущего сигнала.

5.2. УЯЗВИМОСТИ BLUETOOTH

Bluetooth (от слов англ. blue — синий и tooth — зуб) — производственная спецификация беспроводных персональных сетей. Bluetooth обеспечивает обмен информацией между такими устройствами, как персональные компьютеры (настольные, карманные, ноутбуки), мобильные телефоны, принтеры, цифровые фотоаппараты, мышки, клавиатуры, джойстики, наушники, гарнитуры на надёжной, бесплатной, повсеместно доступной радиочастоте для ближней связи.

Bluetooth позволяет этим устройствам сообщаться, когда они находятся в радиусе до 10 м друг от друга (дальность сильно зависит от преград и помех), даже в разных помещениях.

Принцип действия основан на использовании радиоволн. Радиосвязь Bluetooth осуществляется в ISM-диапазоне (англ. Industry, Science and Medicine), который используется в различных бытовых приборах и беспроводных сетях (свободный от лицензирования диапазон 2,4-2,4835 ГГц). В Bluetooth применяется метод расширения спектра со скачкообразной перестройкой частоты (англ. Frequency Hopping Spread Spectrum, FHSS). Метод FHSS прост в реализации, обеспечивает устойчивость к широкополосным помехам, а оборудование недорогое.

Согласно алгоритму FHSS, в Bluetooth несущая частота сигнала скачкообразно меняется 1600 раз в секунду (всего выделяется 79 рабочих частот шириной в 1 МГц, а в Японии, Франции и Испании полоса у́же — 23 частотных канала). Последовательность переключения между частотами для каждого соединения является псевдослучайной и известна только передатчику и приёмнику, которые каждые 625 мкс (один временной слот) синхронно перестраиваются с одной несущей частоты на другую. Таким образом, если рядом работают несколько пар приёмник-передатчик, то они не мешают друг другу.

Этот алгоритм является также составной частью системы защиты конфиденциальности передаваемой информации: переход происходит по псевдослучайному алгоритму и определяется отдельно для каждого соединения. При передаче цифровых данных и аудиосигнала (64 кбит/с в обоих направлениях) используются различные схемы кодирования: аудиосигнал не повторяется (как правило), а цифровые данные в случае утери пакета информации будут переданы повторно.

Протокол Bluetooth поддерживает не только соединение «point-to-point», но и соединение «point-to-multipoint».

Все современные смартфоны оснащаются Bluetooth четвертого поколения – какие-то получают версию 4.0, какие-то 4.1, а некоторые 4.2. Тем временем уже вышла пятая версия «синего зуба».

Данные через Bluetooth 5-ого поколения будут теперь передаваться на максимальной скорости 6,25 МБ/с – раньше было 3,125 МБ/с. В помещениях радиус действия увеличился с 10 до 40 метров, на улице – с 50 до 200 метров. Расходует в 2,5 раза меньше энергии.

5.2.1. Безопасность Bluetooth

Sniffing / Spoofing

В июне 2006 года Авишай Вул и Янив Шакед опубликовали статью, содержащую подробное описание атаки на устройства Bluetooth. Материал содержал описание как активной, так и пассивной атаки, позволяющей заполучить PIN-код устройства и в дальнейшем осуществить соединение с данным устройством. Пассивная атака позволяет соответствующе экипированному злоумышленнику «подслушать» (sniffing) процесс инициализации соединения и в дальнейшем использовать полученные в результате прослушки и анализа данные для установления соединения (spoofing).

Для проведения данной атаки злоумышленнику нужно находиться в непосредственной близости и непосредственно в момент установления связи. Это не всегда возможно. Поэтому родилась идея активной атаки. Была обнаружена возможность отправки особого сообщения в определённый момент, позволяющего начать процесс инициализации с устройством злоумышленника. Обе процедуры взлома достаточно сложны и включают несколько этапов, основной из которых — сбор пакетов данных и их анализ. Сами атаки основаны на уязвимостях в механизме аутентификации и создания ключа-шифра между двумя устройствами.

BlueBorne

Исследователи безопасности из компании Armis обнаружили восемь уязвимостей в реализациях Bluetooth, используемых более чем в 8 млрд. устройств по всему миру. Набор уязвимостей получил название BlueBorne.

По словам исследователей, для эксплуатации проблем злоумышленнику не требуется ни взаимодействие с пользователем, ни сопряжение с целевым устройством. Единственное, что необходимо - это включенный Bluetooth. Уязвимости содержатся в реализациях Bluetooth в Android, iOS, Windows и Linux, затрагивая практически все типы устройств, от смартфонов до IoT-гаджетов и «умных» автомобилей.

Три из восьми уязвимостей BlueBorne оцениваются как критические и позволяют злоумышленникам получить полный контроль над устройством, выполнить вредоносный код или осуществить атаку «человек посередине» (Man-in-the-Middle, MitM). По словам исследователей, ранее выявленные уязвимости в Bluetooth содержались в основном на различных уровнях протокола связи, однако BlueBorne затрагивает реализации протокола, минуя различные механизмы аутентификации, что позволяет получит полный контроль над целевым устройством.

Эксперты Armis проинформировали Apple, Google, Microsoft и сообщество Linux о данных уязвимостях. Разработчики уже готовят патчи, которые будут выпущены в скором времени. Корректирующие патчи будут недоступны для устаревших устройств, которые уже не поддерживаются производителем. По оценкам Armis, число таких устройств составляет 40% или более двух миллиардов по всему миру.

Уязвимости BlueBorne получили следующие идентификаторы: CVE-2017-0781, CVE-2017-0782, CVE-2017-0783 и CVE-2017-0785 (Android); CVE-2017-1000251 и CVE-2017-1000250 (Linux); CVE-2017-8628 (Windows). Уязвимости, затрагивающие iOS, на данный момент не имеют идентификаторов. Уязвимости BlueBorne не затрагивают Android-устройства, использующие технологию Bluetooth Low Energy.

5.3. УЯЗВИМОСТИ IrDA

InfraRed Data Association — IrDA, ИК-порт, инфракрасный порт — группа стандартов, описывающая протоколы физического и логического уровня передачи данных с использованием инфракрасного диапазона световых волн в качестве среды передачи. Является разновидностью оптической линии связи ближнего радиуса действия. Была особо популярна в конце 1990-х начале 2000-х годов. В данное время практически вытеснена более современными аналогами, такими как WiFi и Bluetooth.

Основные причины отказа от IrDA были:

- Усложнение сборки корпусов устройств, в которых монтировалось ИК-прозрачное окно.
- Ограниченная дальность действия и требования прямой видимости пары приёмник-передатчик.
- Относительно низкая скорость передачи данных первых реализаций стандарта. В последующих ревизиях стандарта этот недостаток исправили: скоростные возможности немного превышают, например, возможности самой распространённой на сегодняшний момент версии протокола Bluetooth (спецификация 4.0). Однако широкого распространения скоростные варианты IrDA получить уже не успели.

Аппаратная реализация, как правило, представляет собой пару из излучателя, в виде инфракрасного светодиода, и приёмника, в виде фотодиода расположенных на каждой из сторон линии связи. Наличие и передатчика и приёмника на каждой из сторон является необходимым для использования протоколов двусторонней передачи данных.

В ряде случаев, например при использовании в пультах дистанционного управления бытовой техникой, одна из сторон может быть оснащена только передатчиком, а другая только приёмником.

Технология IrDA уязвима следующим образом:

- яркий свет заглушает сигнал.
- необходима прямая видимость между приемником и передатчиком (или отраженная связь).
- специальные программы для сотовых телефонов могут подделывать и копировать любые сигналы и пульты с IrDA.

5.4. УЯЗВИМОСТИ eTOKEN

eToken (от англ. electronic — электронный и англ. token — признак, жетон) — торговая марка для линейки персональных средств аутентификации в виде USB-ключей и смарткарт, а также программные решения с их использованием.

Функциями смарт-карт обладают все современные модели eToken, за исключением eToken PASS и SafeNet eToken 3500. Функциями USB флэш-накопителей обладают комбинированные устройства eToken NG-FLASH и SafeNet eToken 7300.

Функциями OTP-токенов (устройств для генерации одноразовых паролей) обладают eToken NG-OTP, eToken PASS, SafeNet eToken 3400 и SafeNet eToken 3500.

Аппаратные eToken с функциями смарт-карты можно использовать для интерактивной аутентификации в домене Windows 2000-Server 2008. При наличии на компьютере драйверов eToken рабочий стол аутентификации позволяет не только вводить имя пользователя, пароль и имя домена, как обычно, после нажатия клавиш CTRL+ALT+DELETE, но и вместо нажатия этого сочетания клавиш подключать смарт-карту (eToken) и вводить PIN-код. Кроме того, начиная с Windows XP стало возможным использовать смарт-карты, в том числе eToken, для аутентификации при запуске приложений от имени другого пользователя.

Помимо использования eToken в качестве средства аутентификации, он ещё может использоваться для обеспечения безопасности рабочего места в отсутствие пользователя. Windows 2000–Server 2008 можно настроить таким образом, что компьютер будет блокироваться при отсоединении eToken.

Для использования eToken в качестве средства аутентификации в домене Windows необходим развёрнутый и специально для этого настроенный центр сертификации предприятия (Microsoft Enterprise CA). Средствами eToken генерируется ключевая пара, и центр сертификации выпускает для пользователя сертификат открытого ключа, в котором в политику использования закрытого ключа включён пункт «вход со смарт-картой». После этого администратор может распространить на пользователя объект политики безопасности, запрещающий вход в систему без смарт-карты, в результате чего пользователь не сможет входить в систему без использования eToken, в памяти которого хранится подготовленный сертификат открытого ключа и соответствующий ему закрытый ключ.

Моделям eToken с функциями смарт-карт присущи недостатки, свойственные всем устройствам, в которых PIN-код вводится не с собственной клавиатуры устройства, а с клавиатуры терминала, к которому устройство подключено: с помощью троянской программы злоумышленник может перехватить PIN-код и произвести неоднократное несанкционированное подписывание или шифрование любой информации от имени владельца устройства.

Это может быть троян на компьютере пользователя, микрокамера с хорошим обзором, акустический датчик и другие способы реализации перехвата. Также не стоит забывать про терморектальный криптоанализ. А зная PIN, вытащить секретный ключ не составляет никакого труда – не сложнее, чем скопировать файл (при условии, что токен у злоумышленника).

Из всего этого следует, что краеугольный камень безопасности вашей ЭП при хранении на токене закрытого ключа – PIN-код, и хранить его надо соответственно.

5.5. УЯЗВИМОСТИ ЧИПОВ И RFID-МЕТОК

RFID (англ. Radio Frequency IDentification, радиочастотная идентификация) — способ автоматической идентификации объектов, в котором посредством радиосигналов считываются или записываются данные, хранящиеся в так называемых транспондерах, или RFID-метках.

Любая RFID-система состоит из считывающего устройства (считыватель, ридер или интеррогатор) и транспондера (он же RFID-метка, иногда также применяется термин RFID-тег).

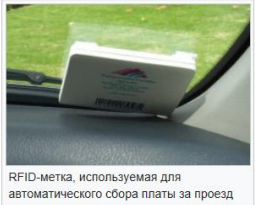
По дальности считывания RFID-системы можно подразделить на системы:

- ближней идентификации (считывание производится на расстоянии до 20 см);
- идентификации средней дальности (от 20 см до 5 м);
- дальней идентификации (от 5 м до 300 м)

Большинство RFID-меток состоит из двух частей. Первая — интегральная схема (ИС) для хранения и обработки информации, модулирования и демодулирования радиочастотного (RF) сигнала и некоторых других функций. Вторая — антенна для приёма и передачи сигнала.


EPC RFID-метка, используемая в торговой сети Wal-Mart


RFID-метка 125 кГц


RFID-метка, используемая для автоматического сбора платы за проезд по платным дорогам (electronic toll collection)


RFID-антенна

С введением RFID-меток в повседневную жизнь связан ряд проблем. Например, потребители, не обладающие считывателями, не всегда могут обнаружить метки, прикреплённые к товару на этапе производства и упаковки, и избавиться от них. Хотя при продаже, как правило, такие метки уничтожаются, сам факт их наличия вызывает опасения у правозащитных организаций и некоторых представителей Русской Православной Церкви.

Уже известные приложения RFID (бесконтактные карты в системах контроля и управления доступом, системах дальней идентификации и в платёжных системах) получают дополнительную популярность с развитием интернет-услуг.

5.5.1. Пассивные RFID-метки

Пассивные RFID-метки не имеют встроенного источника энергии. Электрический ток, индуцированный в антенне электромагнитным сигналом от считывателя, обеспечивает достаточную мощность для функционирования кремниевого КМОП-чипа, размещённого в метке, и передачи ответного сигнала.

Коммерческие реализации низкочастотных RFID-меток могут быть встроены в стикер (наклейку) или имплантированы под кожу (VeriChip).

В 2006 Hitachi изготовила пассивное устройство, названное μ-Chip (мю-чип), размерами 0,15×0,15 мм (не включая антенну) и тоньше бумажного листа (7,5 мкм). Такого уровня интеграции позволяет достичь технология «кремний-на-изоляторе» (SOI). μ-Chip может передавать 128-битный уникальный идентификационный номер, записанный в микросхему на этапе производства. Данный номер не может быть изменён в дальнейшем, что гарантирует высокий уровень достоверности и означает, что этот номер будет жёстко привязан (ассоциирован) с тем объектом, к которому присоединяется или в

который встраивается этот чип. μ-Chip от Hitachi имеет типичный радиус считывания 30 см. В феврале 2007 года Hitachi представила RFID-устройство, обладающее размерами 0,05×0,05 мм, и толщиной, достаточной для встраивания в лист бумаги.

Микросхемы RFID, внедренные в бумагу, из которой изготавливаются банкноты, исключат возможность подделки денег.

5.5.2. Активные RFID-метки

Активные RFID-метки обладают собственным источником питания и не зависят от энергии считывателя, вследствие чего они читаются на дальнем расстоянии, имеют бóльшие размеры и могут быть оснащены дополнительной электроникой. Однако, такие метки наиболее дороги, а у батарей ограничено время работы.

Активные метки в большинстве случаев более надёжны и обеспечивают самую высокую точность считывания на максимальном расстоянии. Активные метки, обладая собственным источником питания, также могут генерировать выходной сигнал большего уровня, чем пассивные, позволяя применять их в более агрессивных для радиочастотного сигнала средах: воде (включая людей и животных, которые в основном состоят из воды), металлах (корабельные контейнеры, автомобили), для больших расстояний на воздухе.

Большинство активных меток позволяет передать сигнал на расстояния в сотни метров при жизни батареи питания до 10 лет. Некоторые RFID-метки имеют встроенные сенсоры, например, для мониторинга температуры скоропортящихся товаров. Другие типы сенсоров в совокупности с активными метками могут применяться для измерения влажности, регистрации толчков/вибрации, света, радиации, температуры и газов в атмосфере (например, этилена).

Активные метки обычно имеют гораздо больший радиус считывания (до 300 м) и объём памяти, чем пассивные, и способны хранить больший объём информации для отправки приёмопередатчиком.

5.5.3. Преимущества радиочастотной идентификации

Возможность перезаписи. Данные RFID-метки могут перезаписываться и дополняться много раз, тогда как данные на штрих-коде не могут быть изменены — они записываются сразу при печати.

Отсутствие необходимости в прямой видимости. RFID-считывателю не требуется прямая видимость метки, чтобы считать её данные. Взаимная ориентация метки и считывателя часто не играет роли. Метки могут читаться через упаковку, что делает возможным их скрытое размещение. Для чтения данных метке достаточно хотя бы ненадолго попасть в зону регистрации, перемещаясь, в том числе, и на довольно большой скорости. Напротив, устройству считывания штрих-кода всегда необходима прямая видимость штрих-кода для его чтения.

Большее расстояние чтения. RFID-метка может считываться на значительно большем расстоянии, чем штрих-код. В зависимости от модели метки и считывателя, радиус считывания может составлять до нескольких сотен метров. В то же время подобные расстояния требуются не всегда.

Больший объём хранения данных. RFID-метка может хранить значительно больше

информации, чем штрих-код.

Поддержка чтения нескольких меток. Промышленные считыватели могут одновременно считывать множество (более тысячи) RFID-меток в секунду, используя так называемую антиколлизионную функцию. Устройство считывания штрих-кода может единовременно сканировать только один штрих-код.

Считывание данных метки при любом её расположении. В целях обеспечения автоматического считывания штрихового кода, комитеты по стандартам (в том числе EAN International) разработали правила размещения штрих-меток на товарной и транспортной упаковке. К радиочастотным меткам эти требования не относятся. Единственное условие — нахождение метки в зоне действия считывателя.

Устойчивость к воздействию окружающей среды. Существуют RFID-метки, обладающие повышенной прочностью и сопротивляемостью жёстким условиям рабочей среды, а штрих-код легко повреждается (например, влагой или загрязнением). В тех сферах применения, где один и тот же объект может использоваться неограниченное количество раз (например, при идентификации контейнеров или возвратной тары), радиочастотная метка оказывается более приемлемым средством идентификации, так как её не требуется размещать на внешней стороне упаковки. Пассивные RFID-метки имеют практически неограниченный срок эксплуатации.

Многоцелевое использование. RFID-метка может использоваться для выполнения других задач, помимо функции носителя данных. Штрих-код же не программируем и является лишь средством хранения данных.

Высокая степень безопасности. Уникальное неизменяемое число-идентификатор, присваиваемое метке при производстве, гарантирует высокую степень защиты меток от подделки. Также данные на метке могут быть зашифрованы. Радиочастотная метка обладает возможностью закрыть паролем операции записи и считывания данных, а также зашифровать их передачу. В одной метке можно одновременно хранить открытые и закрытые данные.

5.5.4. Недостатки радиочастотной идентификации

- Работоспособность метки утрачивается при частичном механическом повреждении.
- Стоимость системы выше стоимости системы учёта, основанной на штрих-кодах.
- Сложность самостоятельного изготовления. Штрих-код можно напечатать на любом принтере.
- Подверженность помехам в виде электромагнитных полей.
- Недоверие пользователей, возможности использования её для сбора информации о людях.
- Установленная техническая база для считывания штрих-кодов существенно превосходит по объёму решения на основе RFID.
- Недостаточная открытость выработанных стандартов.

5.5.5. RFID и права человека

Использование RFID-меток вызвало серьёзную полемику, критику и даже бойкотирование товаров. Четыре основных проблемы этой технологии, связанные с неприкосновенностью частной жизни, следующие:

- Покупатель может даже не знать о наличии RFID-метки. Или не может её удалить.
- Данные с метки могут быть считаны дистанционно без ведома владельца.

- Если помеченный предмет оплачивается кредитной картой, то возможно однозначно связать уникальный идентификатор метки с покупателем.
- Система меток EPCGlobal создаёт или предполагает создание уникальных серийных номеров для всех продуктов, несмотря на то, что это создаёт проблемы с неприкосновенностью частной жизни и совершенно не является необходимым для большинства приложений.

Основное беспокойство вызывается тем, что иногда RFID-метки остаются в рабочем состоянии даже после того, как товар куплен и вынесен из магазина, и поэтому могут быть использованы для слежки и других неблаговидных целей, не связанных с инвентаризационной функцией меток.

Считывание с небольших расстояний также может представлять опасность, если, например, считанная информация накапливается в базе данных, или грабитель использует карманный считыватель для оценки богатства проходящей мимо потенциальной жертвы. Серийные номера на RFID-метках могут выдавать дополнительную информацию даже после избавления от товара. Например, метки в перепроданных или подаренных вещах могут быть использованы для установления круга общения человека.

5.5.6. Уязвимости в RFID-технологии

Угроза вирусов

Исследователи Свободного университета Амстердама создали чип RFID, зараженный вирусом, и таким образом доказали, что, несмотря на крайне малый объем памяти этих дешевых микросхем, они подвержены атакам главных врагов всех компьютеров мира. Проблема состоит не только в том, что зараженный RFID-чип выдает неправильную информацию или вовсе не срабатывает. Считывание при прохождении его через специальные сканирующие ворота может нарушить работу базы данных, обрабатывающей информацию с чипа, утверждают ученые Мелани Райбек (Melanie Rieback), Бруно Криспо (Bruno Crispo) и Эндрю Таненбаум (Andrew Tanenbaum).

«Разработчики RFID-технологий считали, что простое сканирование RFID-маркера не может вызвать изменений серверного программного обеспечения и уж тем более не может использоваться для атаки. К сожалению, они ошибались, – говорится в отчете исследователей. – RFID-маркер может быть заражен вирусом, который затем поразит серверную базу данных, используемую программным обеспечением RFID. Из базы данных вирус легко может распространиться на остальные маркеры». В результате злоумышленники могут, например, с помощью зараженного RFID-чипа вызвать сбой в системе обработки движения багажа в авиакомпании, что приведет к самым серьезным последствиям. Технология позволяет также сеять хаос в базах данных супермаркетов. «Наше исследование – это первый тревожный звонок. Мы хотим, чтобы разработчики RFID-технологий задумались над безопасностью своих систем», – подчеркнул Таненбаум.

Взлом чипа

Поскольку считать информацию с тэгов можно на расстоянии в несколько метров, они представляют явную и прямую угрозу для сохранения ее конфиденциальности. Вот почему защитники гражданских прав и свобод считают, что распространение RFID может привести к недопустимому вторжению в частную жизнь.

Они опасаются несанкционированного использования таких чипов за стенами магазина: злоумышленник, владеющий считывающим устройством, сможет прочесть идентификаторы ваших вещей и использовать полученную информацию против вас (например, взломав базу данных нужного магазина и узнав номер вашей кредитки). Перспективы такой инициативы очевидны: государство сможет узнать о своих гражданах всё. Более того, с помощью радиометок можно организовать тотальную слежку.

Электронные документы

Однако самые серьезные последствия может вызвать считывание данных с личных документов. Паспорта с RFID-чипами, в которых хранится конфиденциальная информация об их владельцах, уже выдают в Соединенных Штатах, в Германии. Такие паспорта в соответствии с рекомендациями Международной организации гражданской авиации получили и граждане Турции.

Особенно широкие масштабы приняла выдача документов с чипами в Великобритании. Исследования показали, что эта страна занимает второе место в мире (после США) по внедрению RFID-технологий. Самое большое распространение технология RFID получила в лондонской системе Oyster Cards (универсальных проездных билетов), которой пользуются 7,2 миллиона англичан. Кроме этого RFID используется здесь в сферах здравоохранения и в военных целях.

Настоящий переполох в Великобритании вызвали успешные результаты эксперимента по копированию биометрических данных, записанных в чип паспорта, который провели эксперты из британской группы NO2ID. Биометрический документ – удостоверение личности, содержащее информацию об уникальных физиологических признаках владельца. Это дву- и трехмерные фотографии, отпечатки пальцев, изображения радужной оболочки глаз. Основным элементом такого документа является RFID-чип, состоящий из микрочипа и антенны для передачи данных. В памяти чипа хранится ее собственный уникальный номер и другая информация – в зависимости от сферы использования. Когда владелец биометрического паспорта попадает в зону регистрации, специальный сканер считывает информацию с метки. Радиус действия RFID-чипа может достигать 100 м.

Эксперты, которые теперь активно критикуют идею внедрения электронных паспортов, публично скопировали из RFID-чипов трех подлинных документов все личные и биометрические данные о владельцах. По сообщению Guardian, на обработку всех паспортов взломщикам потребовалось всего 48 часов, и сделали они это с помощью недорого устройства. Таким образом, они доказали, что подделать, а точнее, скопировать основной элемент паспорта нового поколения не составит труда.

Как «убить» чип?

В таком радикальном действии, как мы уже показали выше, заинтересованы исключительно покупатели, озабоченные тайной своей личной жизни и не желающие, чтобы кто-то незаметно мог узнать, какие трусы-майки на них надеты и какие медикаменты лежат у них в кейсе или сумочке. Правда, в схему некоторых RFID-меток по требованию обществ защиты потребителей сейчас включают средства «усыпления», т. е. временной деактивации, однако такой чип при желании можно «разбудить» незаметно для владельца вещи.

Имеется несколько простых народных средств «убийства» RFID, которые, однако, в жизни часто неприменимы. Например, можно отрезать антенну устройства от собственно чипа, но в случае с одеждой это сделать невозможно, не попортив ткань. Можно также ненадолго засунуть вещь в микроволновую печь, однако «взрыв» чипа часто наносит явный вред купленному предмету.

Созданный немцами миниатюрный RFID-Zapper действует по принципу микроволновки, генерируя электромагнитное излучение, мощность которого позволяет выжечь некоторые электронные компоненты, но оставляет внешнюю оболочку чипа практически неповрежденной. Чтобы сделать «заппер» предельно дешевым, решено было изготовить его на основе одноразовой пленочной фотокамеры со вспышкой, поскольку такие «мыльницы» продают практически повсеместно по бросовой цене. Для генерации импульса служит катушка из медной проволоки. Ее помещают внутрь аппарата на месте фотопленки, после чего корпус камеры закрывается – и «убийца RFID» готов к работе от обычной батарейки.

Как защитить чип?

Индустрия RFID, чтобы успокоить недовольных и облегчить внедрение новой перспективной технологии, разработала новые чипы – так называемые Gen2 («второе поколение»), которые выдают прописанные в них данные лишь в том случае, если ридер отправляет правильный пароль считывания. Кроме того, ридер может передать и другой пароль, «на самоуничтожение», приняв который метка стирает свое содержимое, например, когда покупатель покидает магазин с оплаченным товаром.

На первый взгляд, новая схема выглядит гораздо привлекательней, чем RFID первого поколения, особенно если принять во внимание, что хранимые в чипе и передаваемые в эфир данные защищены шифром от перехвата и использования злоумышленниками. Однако при более пристальном изучении Gen2 выяснилось, что предельная дешевизна чипов-меток сыграла фатальную роль и на самом деле защита новой технологии намного слабей, чем хотелось бы.

Как правило, RFID-метки не имеют собственного источника питания, используя энергию излучения прибора-считывателя. Но когда это происходит, каждая операция вычисления в схеме RFID поневоле видоизменяет электромагнитное поле вокруг чипа. Благодаря этому с помощью нехитрой направленной антенны можно отслеживать и регистрировать динамику потребления энергии чипом, в частности различия в побочных сигналах, излучаемых при приеме правильных и неверных битов пароля. Этого достаточно, чтобы с обычного, особым образом запрограммированного сотового телефона, автоматически вычислять пароль самоуничтожения и «убивать» все попавшие в зону облучения RFID.