Глава 4.

Практические заключения по безопасности.

Прежде чем предложить специфичные механизмы защиты, мы сделаем несколько заключений касательно цены, ограничения ресурсов, а так же требований по быстродействию в дешёвых системах RFID. За основу примем метку ценой 5 центов, не включая ридер и расходы на оконечные базы данных. Однако можно условиться, что ридеры и оконечные системы имеют обширные ресурсы для хранения информации, для вычислений и для связи. Наша базисная метка будет, конечно же, пассивной и, предположим, будет иметь 96 бит памяти. Она должна будет выполнять 100 операций в секунду, и функционировать в среде, сильно насыщённой метками.

Количество тактов, приходящихся на операцию чтения, зависит от рабочей частоты, технологии метки и от множества других факторов. Например, метки, работающие на частоте 915 МГц, должны будут резко менять частоту через каждые 400 мс согласно радиочастотным нормам. Тактовая частота метки может быть как кратной, так и дробной относительно частоты радиообмена. Предположим, что наша номинальная метка будет иметь 10 000 тактов на вычисления, связанные с безопасностью. Конечно, это довольно произвольное предположение, но эта цифра представляет полезный потолок при рассмотрении практических механизмов защиты.

Рассеивание энергии – это ещё один из важных вопросов, касающихся меток, и он так же зависит от технологии, рабочей частоты, механизмов энергетической связи и от многих других факторов. Мы не будем устанавливать пределов рассеивания энергии, хотя этот ограничивающий фактор мог бы быть важным при расчёте вычислений, связанных с секретностью. Удивительно, но для некоторых технологий максимальное рассеивание энергии равно 10 мкВт.

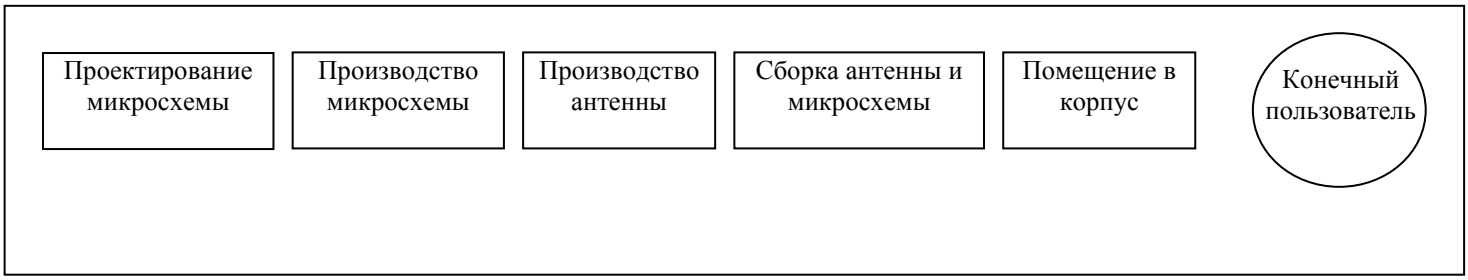

Рис. 4-1: Пять этапов производства метки

Пятью основными этапами в процессе производства РЧ-меток являются: проектирование микросхемы, её производство, производство антенны, сборка антенны/микросхемы, помещение в корпус. Этот процесс изображён на рисунке 4-1. Будем считать, что стоимость проектирования микросхемы фиксирована и

не учитывается в стоимости наших меток. В 2003 году большая часть стоимости метки должна приходиться на изготовление антенны, сборку микросхемы/антенны, а так же на помещение в корпус. Каждый из этих этапов стоит примерно 1 цент и для производства метки остаётся приблизительно 1-2 цента.

На стоимость производства микросхемы главным образом влияет т.н. сырой кремний. Один квадратный миллиметр кремния стоит примерно 4 цента. Многие годы эта стоимость была более или менее стабильна. При такой цене назначенный для базисной метки бюджет позволяет использовать микросхемы площадью максимум 0.25 кв. мм. Количество вентилей на кв. мм. (плотность вентилей) зависит от ширины линии, используемой в технологии производства ИМС. В таблице 4.1 показано типичное соответствие плотности вентилей и стоимости. Данная технология RFID скорее всего будет использовать элементы размером 0.5 или 0.35 мкм. Сделаем свободное предположение, что на проектирование безопасности в базисной РЧ-метке будет отведено 200 – 2000 вентилей. На практике каждые дополнительные 1000 вентилей будут увеличивать стоимость на 1 цент.

Подсчитанное количество вентилей далеко от необходимого для реализации стандартных алгоритмов шифрования с открытым ключом и симметричного шифрования. Фактически только частный ключ для большинства алгоритмов на открытом ключе уменьшают общее пространство. При этом не спасают даже схемы с относительно небольшими ключами, такие как “NTRU” и шифр системы на эллиптических кривых. Симметричные алгоритмы приносят не лучший результат. Аппаратные реализации алгоритмов DES и AES работают на 20 – 30 тыс. вентилях. Эти цифры превышают ресурсы *всего* проекта RFID. Реализация стандартных криптографических хеш-функций, таких как SHA-1, также обходится примерно в 20 тыс. вентилей. Даже имеющий удачное название “Крошечный Алгоритм Шифрования” (Tiny Encryption Algorithm) на сегодняшний день слишком дорог, хотя может пригодиться в скором будущем.

Размер технологии	Вентилей/кв. мм.	Стоимость изготовления, центов/ кв. мм.
0.8 мкм.	1 500	2.5
0.5 мкм.	4 000	3
0.35 мкм.	10 000	4
0.25 мкм.	38 000	6
0.18 мкм.	60 000	8

Таблица 4.1: плотность вентилей и стоимость отливки для нескольких различных технологий.

Как уже обсуждалось в главе 3, элементы памяти метки могут подвергаться физическому вмешательству (согласно контексту главы 3, атакам Филис). Но защита от взлома или физическое экранирование – недопустимо дороги. Вследствие этого нашим меткам нельзя доверять долгосрочное хранение секретной информации.

Отдельным вопросом, возникающим при реализации пассивных РЧ-меток, является *асимметричная сила каналов* (прямого – от ридера к метке – и обратного). Поскольку пассивные метки получают энергию посредством прямого канала, то он намного сильнее обратного. Как результат, прямой канал можно наблюдать с гораздо большего расстояния, чем обратный. Например,

пассивные метки, работающие на частоте 915 МГц, имеют область действия 3 метра, при этом прямой канал прослеживается на протяжении 100 м. Теоретически, в идеальных условиях, 915-мегагерцовый прямой канал ловится на расстоянии одного километра. Эта ситуация представлена на рисунке 4-2.

Асимметрия в силе каналов может привести к подслушиванию, а именно к атаке Евы. Предположим, что в общем лишь прямой канал может прослеживаться без обнаружения. Чтобы иметь доступ к обратному каналу, подслушивающий должен находиться в достаточной близи от метки (например, в 3 метрах). Однако нельзя полностью исключать угрозу прослушивания обратного канала. Ведь у Евы есть возможность расставить подслушивающие устройства или же попытаться установить жучёк на законный считыватель. Однако проведение этих атак обходится более дорого и их легче раскрыть, чем при прослушивании прямого канала.

Алгоритм антиколлизии методом Обхода Бинарного Дерева уязвим вследствие асимметрии сил каналов. Вспомните, что при работе по протоколу обхода дерева, считыватель будет широко вещать каждый бит ИН выделяемой им метки. Потому как при этом используется прямой канал, злоумышленник способен узнать полный ИН, находясь на безопасном расстоянии от считывателя. И потому как выделению подвергаются все метки, у него скоро появится полный список ИН всех читаемых меток. Предложения относительно этой темы представлены в разделе 5.4.

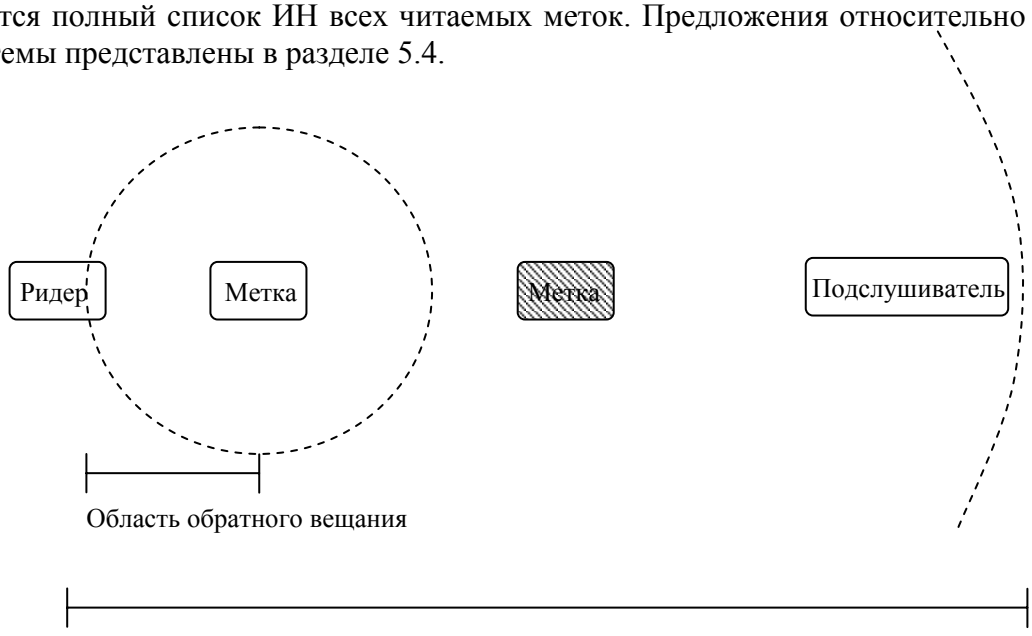

Рис. 4-2: Считыватель может обнаружить лишь ту метку, которая находится достаточно близко от него. Издалека можно подслушать прямой канал, но нельзя получить ответы метки.

Метки, так же как и смарт карты могут быть оснащены физическим каналом связи. Этот канал может быть использован для критичных функций или для *штампования*. Штампование – это процесс установки права собственности на неинициализированное устройство. Штампование метки, скорее всего, будет требовать некоторого времени, а также физического наличия метки. Плюс ко всему мы можем предположить, что метки будут содержать некоторую оптическую информацию, как-то: штрих коды или же обычные цифры. В своём предложении по защите Евро-банкнот, Жуелс и Паппу используют этот метод печатной информации как подкрепление к информации памяти метки.

Предполагается, что метки будут иметь некоторый механизм “отклика”, позволяющий обнаружить их присутствие. Подобное функционирование сродни работе меток класса 0 для электронного наблюдения за товарами (EAS). Кто угодно может окликнуть метку, она же отзовётся некоторым неуникальным сигналом. Также в метках будет реализована команда “деактивации” (“kill”). Деактивация метки будет медленным физическим процессом, походящим на штампование, после чего метка сразу же станет неработоспособной. Метка может быть деактивирована отсоединением антенны, коротким замыканием или подвержением мощному микроволновому излучению. Обобщённо наш проект базисной метки изображён на рисунке 4-3. Предложения, приведённые в главе 5, будут спроектированы с учётом этой спецификации.

- **Метка EPC 1 класса:** пассивное питание, ROM на 96 бит.
- **Радиус:** рабочий – 3м., прямой канал – 100м., обратный – 3м.
- **Антиколлизия:** Детерминистический, либо вероятностный алгоритм.
- **Быстродействие:** 100 операций чтения в секунду.
- **Количество тактов на операцию чтения:** 10 000.
- **Количество вентилей для обеспечения безопасности:** 200 – 2000.
- **Логические операции:** *чтение*, *оклик*.
- **Физические операции:** *штампование*, *деактивация*.

Рис. 4-3: Пример спецификации недорогой РЧ-метки.

Глава 5.

Предложения по защите.

Работая над ограничениями, указанными в главе 4, будем решать вопросы, поднятые в главе 3. Мы заключили, что метки уязвимы для атак на физическом уровне на аппаратную часть. В результате, основными проблемами являются активные атаки и подслушивание. Эти атаки могут быть направлены