Глава 3.

Вопросы безопасности и приватности.

Внедрение RFID-систем даёт огромное преимущество. Но в то же время ставит под угрозу безопасность и приватность. Незащищённым меткам угрожают физическими атаками, подделкой, подслушиванием трафика, атаками вида отказа в обслуживании и т.д.

Каждая из приведённых выше угроз влияет на приватность и безопасность как физических, так и юридических лиц. Согласно традиции, в этой работе ряд возможных атак на системы RFID будет представлен рядом физических лиц:

Эллис, Боб – законные субъекты работы криптографических протоколов;

Дэнис–лицо, проводящее атаки типа отказа в обслуживании;

Ева–лицо, способное лишь на пассивное подслушивание;

Мэлори–злоумышленник, способный сыграть роль законного субъекта;

Филис–злоумышленник, способный нанести физический ущерб аппаратуре системы;

Трейси–злоумышленник, не способный подслушивать, но способный распознать момент отправки сообщений.

3.1. Действующие лица.

Филис: Филис – наиболее сильная злоумышленница. Предполагается, что она способна физически завладеть метками и провести в лабораторных условиях изощренные атаки описанные в [3] и [107]. В арсенал ее атак могут входить зондирование, удаления материала при помощи формового заряда или жидкостного травления, энергетические атаки, отпечатывание излучением, нарушения работы схемы или введения сбоя тактирования.

К счастью, за исключением TEMPEST [71] атак Филис не может проводить атаки открыто или же в широком масштабе. И конечно довольно спорной представляется обеспокоенность безопасностью и приватностью, в то время как Филис вполне может тайком завладеть метками, встроенными в упаковку продукта.

Мэлори: Мэлори не имеет физического доступа к меткам, но может активно участвовать в работе протоколов или же создавать свои собственные поддельные метки. По желанию, Мэлори может сама опрашивать метки или отвечать на запросы ридера.

Ева: Ева играет пассивную роль. Она не может активно вмешиваться в работу протоколов, а способна лишь прослушивать эфир. Она может слышать лишь “логические” послания – ‘1’ и ‘0’, предаваемые в протоколах.

Трейси: Трейси слабее Евы. Трейси не может прочитать содержание посылок, однако всё же способна обнаружить их наличие. Другими словами Трейси может лишь анализировать трафик и определять количество и время прихода сообщений. Трейси может проводить атаки против “области секретности” [9]. В некоторых случаях Трейси может быть столь же опасна, сколь и Ева.

Дэнис: Из всех действующих лиц, Дэнис наиболее слабая. Она не только не может читать сообщения, но деже не способна обнаружить их. Дэнис может лишь помешать вещанию, блокировать сообщения и проводить другие атаки из сферы отказа в обслуживании. По мере того, как RFID приобретает всё большую популярность, ущерб в результате атак Дэнис может увеличиться.

3.2. Угрозы и атаки.

Любая из приведённых выше атак может нести угрозу секретности и безопасности. К примеру, представьте себе розничные товары с незащищёнными метками, которые несёт покупатель. Если в этих метках нет блока управления доступом, то Мэлори может произвольным образом опросить их. На первый взгляд это может показаться неопасным. Кто угодно может случайно заглянуть в вашу тележку в магазине или бросить взгляд в сумку.

Однако обычное подглядывание нельзя осуществить автоматически при желании или в широком масштабе, что вполне может сделать Мэлори. Книги, журналы, медикаменты, нижнее бельё – не многим захочется, чтобы случайные незнакомцы узнали об этих вещах. Кроме надоедливых соседей, дотошные торговцы или воры могут отличить человека по имеющимся у него на руках продуктам.

Представим себе ситуацию, когда информация метки защищается посредством того, что её хранят в базе данных, тогда как непосредственно на карточке записывается указатель на соответствующую запись. Но при этом всё же остаётся вероятность прослеживания лиц, несущих метки. Притом, что метка отзывается одним и тем же значением указателя на любой запрос, её обладателя можно с лёгкостью отследить при помощи некоторого количества ридеров, которые Мэлори установила в пределах некоторой области. Таким образом, нарушается концепция “приватности местонахождения” [9]. Недопустимо автоматическое отслеживание местонахождения людей. Похожие проблемы возникают и в других распространяющихся вычислительных системах, таких, например, как сети “Bluetooth” [51].

Является ли в действительности приватность местонахождения столь важным моментом? Нас постоянно снимают на служебные видеокамеры, которых становится всё больше, и некоторые из которых работают совместно с программами распознавания лица. Кто угодно может проследить ваше передвижение в общественных местах, либо нанять для этого частного следователя. Отличие этих методов от технологии RFID – в том, что отслеживание в последнем случае может производиться автоматически и с большей точностью. И хотя большинству людей может быть всё равно, следят за ними или нет в общественных местах, тем не менее, лицам, больным СПИД, верующим и даже поставщикам продукции секс-шопов может понадобиться защита от подобного автоматического обнаружения.

Рассмотрим случай, когда все уникальные данные метки удаляются из неё при покупке товара. Например, стирается серийный номер, но остаются коды производителя и продукта. Покупатели могут использовать эти коды, и при этом их уже нельзя будет отследить по уникальным серийным номерам. К сожалению, в этом случае Мэлори всё же сможет разоблачить любого, кто несёт “смущающую” продукцию. К тому же комбинации торговых марок могут быть использованы, как уникальные идентификаторы.

Метки, конечно, можно при покупке отключать полностью. Однако нет никаких сомнений, что в скором будущем начнут возникать всевозможные новаторские способы применения RFID для удобства в быту. В качестве примера можно представить себе “умные” аптечки, кладовые для продуктов или холодильники. Для RFID также много места на рынке уничтожения и переработки отходов. Незащищённые метки представляют угрозу секретности не только для частных лиц. Представьте себе супермаркет, в котором устанавливается система “умных полок” и на продажу выставляется продукция, оснащённая метками. В этом случае физические атаки, на которые способна Филис, не принесут много пользы. Можно предположить, что в магазине будет находиться охрана, или будут установлены видеокамеры, при помощи которых можно будет обнаружить физические атаки против оборудования RFID.

Однако Мэлори способна провести нападение на незащищённую систему RFID множеством способов. При отсутствии у меток контроля доступа по чтению, Мэлори может провести опрос всех товаров в магазине. Путём проведения периодического сканирования, Мэлори может получить информацию о продажах; если эта информация будет достаточно ценной, Мэлори может начать работу в качестве корпоративного шпиона.

Мэлори может действовать иным образом и заменить данные меток дорогих товаров на содержимое меток дешёвых. Похожие атаки можно провести против штрих кодов. На одном веб-сайте [77] даже хранилась база данных наклеек со штрих кодами (хотя он был закрыт в течение недели).

В то время как проницательный служащий может обнаружить поддельную наклейку на упаковке, Мэлори при помощи беспроводной связи спокойно переписывает незащищённую метку. После этого она может уйти из магазина, вернуться безо всяких обличающих её пишущих устройств и правдиво заверять, что ничего не могла поделать с разладившимися РЧ-метками. С другой стороны, начала применяться практика маркировки предметов роскоши при помощи меток [79]. Теперь Мэлори может записывать информацию с настоящих ценностей на дешёвые подделки.

Кроме подлога, Мэлори так же может облегчить кражу. Допустим, в магазине установлена система автоматического контроля, – покупатели оплачивают товар, не вынимая из сумки, когда они выходят из магазина. “Умные” полки при этом будут отслеживать, когда товары покинули полки. При этом вызывается охрана, если обнаруживается, что покинувший полку товар в течение некоторого периода времени не был вынесен из магазина.

Так как Мэлори способна подделывать метки, она может обмануть систему автоматического контроля. Мэлори может взять товар с полки и поместить его в пролинованную металлом сумку. Подобная продукция уже существует на рынке [68]. Исчезновение продукта естественно будет регистрироваться как аномалия. Однако Мэлори может заменить его устройством-ловушкой, подражающим метке-оригиналу. При этом полка будет

“думать”, что продукт вернули на место, и Мэлори сможет беспрепятственно уйти из магазина. Мэлори может даже создать одно устройство, способное имитировать насколько меток одновременно.

Подобные *имитационные атаки* также срабатывают против работающих по технологии RFID автозаправочных систем типа E-ZPass [32], или в турникетах метро. У Мэлори есть преимущество, поскольку её устройства-имитаторы не имеют тех же физических и стоимостных ограничений, как системы RFID. В то время как метки, используемые в магазинах, должны быть дешёвыми и легко вделываемыми в продукцию, Мэлори может создать активное, более объёмное устройство. И пока устройства-имитаторы будут стоить меньше, чем некоторые товары, всегда будет существовать стимул для воровства.

Хоть Ева и слабее, чем Мэлори, она всё же может представлять значительную угрозу безопасности и секретности. Ева не способна случайным образом опрашивать метки, но она может “встать” рядом с законным ридером и подслушивать. Например, Ева может ждать у выхода из аптеки, вблизи от турникета метро или ещё где-нибудь, где метки можно прочитать при помощи авторизованного ридера. Тем же путём Ева может заниматься промышленным шпионажем. Записывая сигналы опроса меток в магазине, Ева может получить ту же информацию, которую приносили активные атаки Мэлори.

Даже Трейси несёт угрозу безопасности и секретности. Хоть она и не может опрашивать метки или подслушивать, она всё же способна определить присутствие самих меток и сигналов их опроса. И в этом случае людей можно идентифицировать по количеству имеющихся у них меток (особенно по их необычно большому числу). Трейси может даже постепенно собрать информацию об инвентаре. Например, то, что ридер в производственном секторе опрашивает x меток, и что в прибывшем грузовике с молоком было y меток – это хоть и не точная, но всё же ценная информация.

Самая слабая, Дэнис, также представляет угрозу. Дэнис не может извлечь полезную информацию из системы RFID, но, тем не менее, может провести атаку типа отказ в обслуживании. Она способна заполнить радиочастотные каналы шумом и подорвать или фальсифицировать связь. Дэнис могла бы даже провести низкоуровневую атаку направленной энергией, чтобы уничтожить метки. Аналогичным образом кто-то может с лёгкостью уничтожить штрих коды, сотря их или записав поверх них. Так или иначе, Дэнис может автоматически нарушить работу систем RFID в широком масштабе посредством радиочастот.