А. В. Стариковский, Д. М. Михайлов

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ БЮДЖЕТНЫХ RFID-МЕТОК С ИСПОЛЬЗОВАНИЕМ СПЕЦИАЛЬНОГО ОБЛЕГЧЕННОГО ПРОТОКОЛА АУТЕНТИФИКАЦИИ

Введение

RFID-метки являются составной частью системы радиочастотной идентификации (RFID), которая включает в себя набор меток и RF-сканер. Метки, о которых идет речь в данной статье, состоят из антенны и соединенного с ней микрочипа. Использование микрочипов на кремниевой основе позволяет внедрять в них определенный набор функций, включая перезаписываемое хранилище данных и небольшой набор вычислительных возможностей. RF-сканеры излучают радиочастотные сигналы для получения информации, которая хранится в RFID-метках. Эта информация может варьироваться от статичных идентификационных номеров до записываемой пользователем или вычисляемой метками информации.

Бюджетные RFID-метки, используемые в магазинах в качестве «умных ярлычков», фактически являются более экономичной и эффективной заменой оптических штрих-кодов. К преимуществам RFID-меток можно отнести автоматическое считывание информации с меток, находящихся вне поля зрения, через непроводящие материалы, с частотой несколько сотен меток в секунду и с расстояния нескольких метров. Другими сферами, в которых могут быть полезны бюджетные RFID-метки, являются, например, сельское хозяйство, автомобильная промышленность, контроль доступа в здания, инвентаризация и т. д. Из-за многочисленных сфер применения и низкой стоимости меток RFID-технологии имеют все возможности для того, чтобы стать повсеместно используемыми и востребованными.

Тем не менее в многочисленных работах ученых указывается на то, что универсальное применение систем радиочастотной идентификации RFID может создать новые проблемы информационной безопасности. Потенциальные риски включают промышленный шпионаж, вторжение в частную жизнь и собственность потребителей. В традиционных вычислительных системах многие проблемы информационной безопасности могут быть решены использованием криптографических методов [1]. К сожалению, RFID-метки значительно ограничены в ресурсах и не могут поддерживать мощную криптографию. Если затрагивать коммерческую составляющую внедрения RFID-меток, то можно говорить о том, что метки теоретически могут иметь встроенные средства для поддержки криптографических методов защиты и другие возможности повышения информационной безопасности, но при этом стоимость RFID-меток возрастет в 10—50 раз [2]. Подобное возрастание стоимости переведет RFID-метки в категорию специфических, дорогих решений, которые уже не смогут широко использоваться.

Возвращаясь к бюджетным RFID-меткам, перечислим характеристики, которыми они обладают:

- емкость в несколько сотен бит;
- несколько тысяч вентилей, доступных для реализации логических функций;
- энергонезависимость, что исключает фоновые вычисления в момент простоя, когда метка не «питается» от RF-сканера;
- ограниченный радиус действия и качество радиопередачи из-за слабой приемной антенны и жесткие ограничения по мощности меток;
- отсутствие защиты от повреждений.

Отметим, что внедрение даже стандартной криптографической хеш-функции, такой как MD5 или SHA-1, невозможно для бюджетных RFID-меток. Таким образом, имеет место острая

потребность в новых, облегченных криптографических элементах, которые будут поддерживаться бюджетными RFID-метками.

В статье описан облегченный протокол с аутентификацией типа «запрос-подтверждение», который может быть использован в бюджетных RF-системах для аутентификации меток. Аутентификация меток — важный элемент, который является базовой частью усовершенствованных защитных систем. Примером может служить система защиты от воровства, где RFID-метки прикреплены к защищаемым объектам, а RF-сканер периодически излучает и проводит аутентификацию каждой метки. Система должна быть разработана таким образом, чтобы отсутствовала возможность кражи путем установки клона метки так, что RF-сканер мог бы продолжать обнаруживать метку и не замечать подмены.

2. Системная модель

В статье рассматривается система, состоящая из одного RF-сканера и нескольких RFID-меток. Предполагается, что каждая метка имеет со сканером общий ключ, который создается защищенным способом перед началом работы системы. Метки имеют пассивное питание, поэтому они могут работать только тогда, когда сканер обеспечивает их необходимой для этого энергией. Помимо этого, как уже отмечалось ранее, метки ограничены в ресурсах: они имеют ограниченные вычислительные возможности, ограниченный объем хранения данных и ограниченные способности коммуникации.

Предполагается, что RF-сканер регулярно опрашивает метки, каждый раз с новым запросом, и RFID-метки должны идентифицировать себя путем правильного ответа на запрос. Известны протоколы, которые делают это в защищенном режиме, но они используют стандартные криптографические элементы (MAC, цифровая подпись, шифрование), которые невозможно использовать для бюджетных RFID-меток, поскольку обработка даже стандартной хеш-функции, такой как MD5 или SHA-1, превышает возможности меток и недопустима в рассматриваемой системе. В то время как в случае использования стандартной криптографии скорость и простота алгоритма обычно являются определяющими факторами, в рассматриваемой системе первостепенную важность имеет невысокая сложность элементов.

Задача злоумышленника — создать правильный ответ RFID-метки на запрос RF-сканера. В случае если это происходит, можно утверждать, что протокол скомпрометирован. Данные, из которых злоумышленник пытается подготовить правильный ответ, могут быть получены как пассивным, так и активным путем. В случае пассивной атаки злоумышленник собирает сообщения из одного или нескольких прогонов, не прерывая связи между сканером и меткой. В случае активной атаки злоумышленник имитирует сканер и/или метку и повторяет намеренно измененные сообщения, просмотренные при предыдущих прогонах протокола.

3. Улучшенный протокол аутентификации на основе логической операции XOR

Для начала следует проиллюстрировать некоторые понятия на примере несложного протокола, который использует два различных ключа в обоих направлениях:

$$R \to T : x \oplus k_1, \quad (1)$$

$$T \to R : x \oplus k_2. \quad (2)$$

В формулах (1) и (2) R и T — RF-сканер и RFID-метка соответственно; k_1 и k_2 — секретные ключи R и T; x — случайный запрос длиной n бит.

Безопасность этого протокола была бы доказана, если бы k_1 и k_2 однозначно выбирались случайным образом в каждом прогоне. Тем не менее это ведет к проблеме создания ключа, связанной с особенностями системной модели (ограниченная емкость меток, невозможность частого обновления ключа вручную и т. д.). Для решения проблемы требуется усовершенствованная схема безопасного алгоритмического ключа, которая может быть основана на шифре Вернама.

Однако шифр Вернама позволяет отсылать только те случайные биты, которые используются для передачи сообщения.

Для обновления ключа с использованием логической операции XOR существует следующая возможность: R случайно выбирает в прогоне i новый ключ $k^{(i)}$, шифрует его с помощью логической операции XOR вместе с ключом $k^{(i-1)}$, использованным в предыдущем прогоне. Это приводит к следующему протоколу:

$R \to T : a^{(i)} = x^{(i)} \oplus k^{(i)}, k^{(i)} \oplus k^{(i-1)}$,

$T \to R : b^{(i)} = x^{(i)} \oplus k^{(0)}$,

где $i = 2, 3, \ldots$ — счетчик, содержимое которого увеличивается на единицу с каждым новым прогоном, $x^{(i)}$ — i-й запрос, а $k^{(0)}$ и $k^{(1)}$ — исходные секретные ключи. Этот протокол использует только логические операции XOR, что с точки зрения простоты алгоритма является идеальным решением. Тем не менее он может быть скомпрометирован после двух последовательно просмотренных прогонов. Необходимо изменить протокол, основанный только на XOR. Модифицированный протокол можно записать в следующем виде:

$R \to T : a^{(i)} = x^{(i)} \oplus k^{(i)}$,

$T \to R : b^{(i)} = x^{(i)} \oplus k^{(0)}$,

где $k^{(i)} = \Pi\ (k^{(i-1)})$ и $\Pi : \{0; 1\}^n \to \{0; 1\}^n$ — перестановка, которая используется для усложнения ключа $k^{(0)}$. Π определяется следующим образом. Если предположить, что длина ключа — 128 бит ($n = 128$) и каждый байт $k^{(i-1)}$ делится на два полубайта, то левые полубайты $k_{1,L}^{(i-1)}, k_{2,L}^{(i-1)}, \ldots k_{16,L}^{(i-1)}$ объединяются в вектор, обозначаемый $k_L^{(i-1)}$, а правые полубайты $k_{1,R}^{(i-1)}$, $k_{2,R}^{(i-1)}, \ldots k_{16,R}^{(i-1)}$ — в вектор, обозначаемый $k_R^{(i-1)}$. Далее расчет состоит из двух шагов:

Шаг 1: Элементы $k_R^{(i-1)}$ переставляются, и эта перестановка контролируется $k_L^{(i-1)}$. Результатом является $k_R^{(i)}$.

Шаг 2: Элементы $k_L^{(i-1)}$ переставляются, и эта перестановка контролируется $k_R^{(i-1)}$. Результатом является $k_L^{(i)}$.

$\Pi(k^{(i-1)}) = k(i)$ получается из реорганизации векторов полубайтов $k_L^{(i)}$ и $k_R^{(i)}$ в вектор $k^{(i)}$.

На первом и втором шагах осуществляются следующие операции: первый и $k_{1,L}^{(i-1)}$ элементы вектора $k_R^{(i-1)}$ переставляются местами. Далее переставляются местами второй и $k_{2,L}^{(i-1)}$ элементы вектора, полученные после первой операции. И так до 16-й операции, когда переставляются местами 16-й и $k_{16,L}^{(i-1)}$ элементы, полученные после 15-й операции. Например, $(k_L^{(i-1)}, k_R^{(i-1)}) = ((3, 2, 4, 1), (2, 4, 1, 3))$ преобразуется в $(k_L^{(i)}, k_R^{(i)}) = ((4, 1, 3, 2), (2, 4, 3, 1))$.

Пассивная атака. Просматривая сообщения i и $(i+1)$ прогонов протокола, злоумышленник может вычислить:

$$k^{(i)} \oplus k^{(0)} = a^{(i)} \oplus b^{(i)}, \quad (4)$$

$$k^{(i+1)} \oplus k^{(0)} = a^{(i+1)} \oplus b^{(i+1)}. \quad (5)$$

Объединяя уравнения (4) и (5), он получает:

$$k^{(i)} \oplus k^{(i+1)} = a^{(i)} \oplus a^{(i+1)} \oplus b^{(i)} \oplus b^{(i+1)}, \quad (6)$$

где правая часть известна злоумышленнику. Это означает, что злоумышленник может увидеть разность между последовательными ключами сессий. Его цель — найти начальное число $k^{(0)}$, чтобы имитировать T.

Предположим, что злоумышленник подобрал ключ сессии $k^{(i)}$, $i \geq 1$. Тогда, согласно уравнению (6), он также узнает новый код сессии $k^{(i+1)}$. Он может проверить свое предположение, вычислив $k^{(i+1)}$ из вектора $k^{(i)}$, используя перестановку Π. Тем не менее подбор ключа сессии — это атака грубой силой (brute force), которую можно значительно усложнить увеличением количества прогонов протокола.

Заключение

Цель разработчика облегченных протоколов аутентификации для бюджетных RFID-меток заключается в разработке такого протокола, который имеет доказанную защиту от рассмотренной модели атаки злоумышленника. Доказательство защиты может быть основано на теории (например, шифр Вернама) или на сведении проблемы взлома протокола к математической задаче, которая трудноразрешима. К сожалению, защита такого типа имеет свои недостатки. Так, например, шифр Вернама имеет известную всем проблему управления ключами. В то же время протоколы, которые основаны на громоздких математических вычислениях, требуют огромного количества ресурсов от всех участников процесса.

Следуя основной цели, в статье предложен протокол, основанный исключительно на базовых элементах, которые могут поддерживаться бюджетными RFID-метками, проведен анализ стойкости протокола по отношению к некоторым характерным видам атак. Безусловно, рассмотренный протокол может быть скомпрометирован, однако задача состоит не в предотвращении этого, а в поиске нижней границы сложности протокола для обеспечения требуемой безопасности бюджетных RFID-меток.

Это позволит разработчикам изменять параметры защиты в поисках компромисса между безопасностью RFID-меток и их эксплуатационными качествами. Так, например, зная нижнюю границу, можно выбирать наименьшую возможную частоту обновления ключей.

СПИСОК ЛИТЕРАТУРЫ:

1. *Иванов М. А.* Криптографические методы защиты информации в компьютерных системах и сетях. М.: КУДИЦ-ОБРАЗ, 2001.
2. *Sarma S., Weis S., Engels D.* Radio-frequency Identification: Security Risks and Challenges // CryptoBytes. 2003. V. 6. № 1. P. 2–9.