СПИСОК ЛИТЕРАТУРЫ

1. Котляр Л.В. Принципы и требования к оценке инвестиционной привлекательности региона//Социально-экономические и технические системы. Онлайновый электронный научно-технический журнал, г. Набережные Челны, КамПИ, № 4(12), 2005.

«ЗАКРЫТОЕ» СОСТОЯНИЕ МЕТКИ, КАК СРЕДСТВО ЗАЩИТЫ ОТ НСД В МОДЕЛИ СИСТЕМЫ РАДИОЧАСТОТНОЙ ИДЕНТИФИКАЦИИ

Лайков Ю.М.
ООО «Ридер»,
Москва

При обмене информацией между считывателем и меткой в системе радиочастотной идентификации имеет место угроза извлечения полезных данных из радиоканала, идущего от метки. Кроме того, уникальный номер метки может быть получен в результате несанкционированного опроса в общественном месте.

Для решения этих проблем была построена и отлажена модель на языке поведенческого описания аппаратуры (Verilog), в которой были реализованы стандартные алгоритмы работы радиочастотной системы и введён элемент защиты, описанный ниже. Данный элемент представляет собой дополнительный режим работы метки, находясь в котором она передаёт свой уникальный номер в эфир в засекреченном виде, и только лишь авторизованный считыватель имеет возможность точно идентифицировать метку. Такой режим назван «Закрытым» или «Запертым» состоянием. Соответственно обычный режим обозначается как «Открытое» состояние метки. Переключение метки между этими состояниями осуществляется при помощи специальных команд, содержащих её уникальный номер. Засекреченные номера меток, находящихся в закрытом состоянии, передаются в эфир в виде специальных шифр-векторов, в ответ на запрос считывателя.

Шифр-вектора имеют следующий вид:

$S = R \mid (DynamicHash(R,K)\ xor\ (ID \mid StaticHash(ID)))$

где

R – случайный 32-разрядный двоичный вектор, генерируемый меткой «на лету»;

K – собственный 32-разрядный секретный ключ метки, прошитый в её память на этапе изготовления, либо единожды, в однократно записываемую память;

ID – уникальный 96-разрядный номер метки, прошиваемый на этапе изготовления метки;

DynamicHash(R, K) – 128-разрядный результат вычисления некоторой хеш-функции от R и K(вычисляется «на лету» в процессе антиколлизии);

StaticHash(ID) – 32-разрядный результат вычисления некоторой хеш-функции, возможно отличной от DynamicHash, взятой от ID – либо вычисляется до производства метки и прошивается во время её изготовления наряду с ID, либо вычисляется после того как метка будет изготовлена и прошивается в однократно записываемую память;

| - конкатенация векторов;

xor – двоичное сложение по модулю 2.

Предполагается, что авторизованный считыватель будет «знать» вид функций DynamicHash и StaticHash, а так же держать в своей памяти либо иметь доступ к списку секретных ключей {K1,…,Kn} меток той группы, с которой он должен работать.

После приёма S считыватель

1) выделит R и DS = (DynamicHash(R,K) xor (ID | StaticHash(ID)));

2) начнёт перебирать все известные ему ключи меток Ki, вычислять

Dyni = DynamicHash(R,Ki);

3) Dyni будут складываться по модулю 2 с DS (Stati = Dyni xor DS);

4) полученный вектор Stati будет разбиваться на 2 части (IDi и StHshi);

5) перебор ключей прекратится в том случае, если будет выполнено тождество:

- StHshi = StaticHash(IDi),

- соответственно IDi и будет уникальным номером метки, от которой была получена последовательность S.

Отсюда видно, что ИН метки всё же можно получить перебором (этот процесс можно ускорить, если некоторые биты искомого уникального номера известны), однако это займёт несколько минут, что неприемлемо в случае, когда анализ проводится «на ходу» (например, сканируются метки проходящих мимо считывателя людей). Кроме того, при «удлинении» K, каждый дополнительный бит приведёт к удвоению времени перебора.

Приведённая модель представляет собой новый, более защищённый, при учёте жёстких ограничений по ресурсам радио-меток, вариант описания системы радио-идентификации, позволяет виртуально тестировать данную систему, и при некоторой доработке может быть реализована в готовых устройствах.

«CLOSED» STATE OF REDIO-TAGS AS AN UNAUTHORIZED ACCESS PROTECTION REMEDY IN RADIO FREQUENCY IDENTIFICATION (RFID) SYSTEM MODEL

Laykov Y.M.
“Reader” ltd,
Moscow

There is a threat of valuable data leak from tag’s radio channel during an interchange between a reader and a tag in RFID system. Besides, a tag’s unique identification number (ID) can be obtained as an outcome of unauthorized query of the tag in a public place.

As a solution to the problems a hardware description language (Verilog) model has been built and debugged. Standard RFID system’s algorithms and a new security element are implemented in the model. The security element represents an additional tag’s operation mode. When a tag is in this mode, it broadcasts the ID in a secret form that can be precisely identified only by authorized reader. This mode is named “Closed” tag’s state. A common operation state of a tag is called “Opened” mode respectively. Switching the states is performed by applying particular commands from reader that include the tag’s ID.