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 | (DynamicHash(R,K) xor (ID | 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.

As a response to a reader's query, secret IDs of the tags in a closed state are broadcasted as specific cipher-vectors.

The cipher-vectors have the following form:

S = R | (DynamicHash(R,K) xor (ID | StaticHash(ID)))

where

R – random 32-bit vector generated by a tag "on-the-run";

K – a tag's unique 32-bit secret key, that is written to the tag's ROM during manufacture;

ID – a unique 96-bit identification number of a tag, that if written to its ROM during manufacture;

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

DynamicHash(R, K) – 128 bit result of some hash function calculation that takes R and K as arguments. The function is calculated "on-the-run" bit-by-bit during anti-collision.

StaticHash(ID) – 32-bit result of a particular hash-function calculation that takes ID as an argument. The function is calculated during the manufacture and the result is written to the tag's ROM as it is done with ID;

| - concatenation of vectors;

xor – bit-by-bit XOR.

Assume that a legal reader will be "aware" of DynamicHash and StaticHash forms. The reader's memory will contain a list of secret keys {K1,…,Kn} of the supported tags' group, or the reader will have an access to a database containing this list.

On reception of S a reader shell:

1) separate R and DS = (DynamicHash(R,K) xor (ID | StaticHash(ID)));

2) start sweeping all known tags' keys Ki and evaluating Dyni = DynamicHash(R,Ki);

3) during one sweep Dyni and DS shall be XORed (Stati = Dyni xor DS);

4) the Stati shall be split into IDi and StHshi;

5) the keys search shell stop as soon as the following identity becomes true:

- StHshi = StaticHash(IDi),

- thereafter IDi will represent a unique identifier of the tag that has sent the S sequence.

Hence it is clear that an ID of a tag can still be obtained by searching (this process can be quickened in the case that an adversary knows some bits of the needed ID), however this may take several minutes, which is unacceptable in the case of on-the-run analysis (for example when tags of passing by people are scanned). Besides, if K is "lengthened", every additional bit will lead to doubling the search time.

The model given represents a new, more secure under conditions of harsh radio-tag resource restrictions, alternative of RFID system description. It enables a virtual testing of the system given and, after appliance of some modifications, can be implemented in complete devices.

ПРИМЕНЕНИЕ МЕХАНОХИМИЧЕСКОЙ АКТИВАЦИИ КОМПОНЕНТОВ ВЯЖУЩИХ, ИСПОЛЬЗУЕМЫХ В ЭНЕРГЕТИЧЕСКОМ СТРОИТЕЛЬСТВЕ, КАК ЭФФЕКТИВНЫЙ ВАРИАНТ ЦЕЛЕНАПРАВЛЕННОГО ИЗМЕНЕНИЯ ИХ ФИЗИКО-ХИМИЧЕСКИХ И ТЕХНОЛОГИЧЕСКИХ СВОЙСТВ

Оголь В.Г., Кулебакин В.Г.

Институт химии и химической технологии СО РАН, Красноярск

Энергетика – область промышленности, объекты которой эксплуатируются в диапазоне от отрицательных температур (плотины гидроэлектростанций зимой) до достигающих 1273 К (обмуровка деталей котлов на ТЭС). Из этого вытекает и многообразие используемых в ней строительных материалов и изделий, в том числе, тепло- и гидроизоляционных, бетонов и наполнителей в их составах, вяжущих и т.п. На примере приводимого ниже перечня марок бетонов это очень очевидно: атмосферостойкий, гидротехнический, цементобетон, цементоизвестковый, полимерный, полимерно-цементный, известково - шлаковый, гипсовый, конструктивно - теплоизоляционный, шлакобетон, вермикулитобетон, кварцмулитовый, жаростойкий, в т.ч. огнеупорный, жароупорный, бетоношамот. Жаропрочные бетоны, применяемые например, для газотурбинных установок, должны сохранять высокую длительную прочность (от 100 до 200 МПа) при температурах около 1200 К.

Приведенное перечисление бетонов далеко неполное. Если гидротехнические сооружения типа плотин, построенных 50-100 лет назад, постепенно выходят из строя из-за сезонных, суточных перепадов температур, давления, влажности, постоянного контакта с водой, как в виде жидкости, так и льда, кислотных дождей и т.п., то футеровка (обмуровка) защищаемых участков тепловых агрегатов – из-за усталости теплоизоляции, неоптимальности её рецептуры и, в частности, связующих в её составе.

В связи с этим повышение сроков службы указанных объектов, эффективное «залечивание» поверхностных слоёв инъецированием гидропроникающей изоляции в случае, например, плотин, (принципиальная возможность чего показана и нами [1]), разработка эффективных способов уплотнения смесей для получения целевых продуктов, новых рецептур теплоизоляционных материалов и модифицирование существующих для тепловых агрегатов является задачей чрезвычайной важности. Некоторые способы ее решения известны: подбор фракционного состава компонентов бетонов, неформованных огнеупорных смесей и т.п. по так называемым идеальным кривым распределения для получения наиболее плотной упаковки, укладка материалов методом зонного нагнетания, получение особо плотных изделий формованием и спеканием при введении в них TiO_2 (при этом резко уплотняется обожженная массв) и др.

Предлагаемое нами решение по достижению более высокого уровня технологии подготовки связующих и отдельных компонентов, входящих в их состав, состоит в применении механохимической активации (МА) как отдельных компонентов, так и смесей вя-