МЕТОДИКА ЗАЩИТЫ RFID-МЕТОК ОТ АТАК КОПИРОВАНИЯ И РЕТРАНСЛЯЦИИ

Ворожцов А.О., студент гр.461402

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Пухир Г.А.– старший преподаватель каф. ЗИ

Аннотация. Метки типа RFID, в силу передачи данных по радиоканалу, уязвимы к атакам вида relay и replay. Для предотвращения использования нарушителем перехваченных данных предлагается дополнительный метод определения подлинности карты. Антенна карты меняется на печатную щелевую, со случайным расположение щелей, формирующим уникальный паттерн плотности магнитного поля.

Ключевые слова: RFID, HF, UHF, антенна, диаграмма направленности, плотность магнитного поля, Matlab, Relay-атака, Replay-атака, щелевая антенна.

Введение. В настоящее время довольно активно используются бесконтактные идентификаторы типа RFID. Данные идентификаторы диапазонов HF (13,56МГц) и UHF (865–868МГц в Европе и 902–928МГц в США) применяются в большом количестве областей, как то СКУД, маркировка товаров, общественный транспорт, логистика и многое другое. Для защиты чаще всего применяется симметричное шифрование, передача ранее записанных случайных чисел и измерение времени приёмопередачи. Данные средства защиты частично обходятся методами атак по побочным каналам или уязвимостями, заложенными производителями, что создаёт угрозу информационной безопасности [1].

UHF метки взяты в силу большего возможного разброса коэффициента отражения и меньшей длины волны по сравнению с метками HF диапазона. Так как при вышеупомянутых атаках устройство злоумышленника, будь оно специализированным или универсальным для работы с радиоэфиром, выдаёт себя за терминал, то в основном применяются методы защиты, использующие информацию, которую злоумышленник не может знать.

Предлагается добавление дополнительного физического идентификатора подлинности: антенна метки меняется на печатную щелевую антенну со случайным расположением щелей, таким образом получая уникальную диаграмму напряжённости магнитного поля. Изменением размеров и положения щелей на покрытии возможно получить значительное количество различных паттернов, с разной энтропией, градиентом и коэффициентом отражения. Так как работа ведётся в ближней зоне, то диаграмма направленности не имеет большого значения, и основные вариации будет иметь именно магнитное поле. Терминал оснащается антенной решёткой, позволяющей измерить плотность магнитного поля в разных точках пространства и вспомогательным контроллером, рассчитывающим градиент и коэффициент отражения для несущей частоты [2]. Данные значения передаются основному контроллеру, для ускорения процесса возможно привязать данные значения к ключу шифрования некоторой функцией, уникальной для каждой метки.

Расчёты проводились в САПР Matlab, на базе которого возможно создать приложение, рассчитывающее некоторое количество чертежей антенн с достаточной уникальностью для однозначной идентификации метки. Алгоритм создаёт по заданной чувствительности приёмной антенны и количеству чертежей или характеристикам щелей списки щелей с их расположением и характеристиками, при которых данные комбинации возможно различить на заданном терминале.

Для обхода данной методики защиты помимо длительного контакта с меткой, потребуется наличие оборудования, способного измерить характеристики антенны, ПО для расчёта антенны по данным характеристикам и оборудования для создания идентичной антенны. В силу этого, для проведения атаки нарушитель должен иметь значительный уровень подготовки и материально-технического обеспечения.

Полученный метод позволяет более определять подлинность RFID меток на физическом уровне, без изменения протокола, контроллеров метки и терминала, требуя лишь изменения антенны метки, антенны терминала и установки вспомогательного контроллера. Данный метод применим к любым картам диапазонов HF и UHF, обеспечивая бюджетную и эффективную защиту.

Список использованных источников:

1. Таненбаум А. Эволюция безопасности RFID//IEEE Security & privacy. – 2006. – Т.4, № 2. – С. 62–69.

2 В.В. Муравьев, А. А. Тамело, Д. Ф. Молодкин, Д. Б. Владимиров (2010) Расчёт и проектирование антенн и устройств СВЧ. – Минск, БГУИР.