УДК 004.056.53

МЕТОДИКА ОПРЕДЕЛЕНИЯ ПОДЛИННОСТИ RFID-МЕТОК

А.О.Ворожцов
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

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, с о 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.

METHOD OF DEFINING THE RFID TAGS IDENTITY

A.O. Voroztsov
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. RFID tags, due to usage of radio channel to transmit data, are vulnerable to Relay and Replay types of attacks. To prevent intruder from using captured data, an additional

identification method is proposed. Antenna is changed to slot PCB antenna with random slot positioning, that forms unique pattern of magnetic field density.
Keywords: RFID, HF, UHF, antenna design, radiation pattern, magnetic field density, Matlab, Relay-attack, Replay-attack, slot antenna.

Введение

В настоящее время довольно активно используются бесконтактные идентификаторы типа RFID. Данные идентификаторы имеют широкое применение в областях, где требуется быстрое получение информации с метки. Чаще всего применяются программные методы, вида шифрования, реализованного на метке, передачи ранее записанных случайных чисел, замеры времени для предотвращения Relay-атак. В данной работе предлагается добавление дополнительного физического идентификатора подлинности, который будет более дорогим и трудоемким для подделки. Основной фокус идет на метки диапазона UHF—856-868 и 902-928 МГц для Европы и США соответственно, но может быть применен и к меткам диапазона HF–13,56 МГц.

Основная часть

UHF и HF идентификаторы применяются в большом количестве областей, как то СКУД, маркировка товаров, общественный транспорт, логистика и многое другое. UHF метки часто применяются для маркировки товаров, в силу хорошей электромагнитной совместимости и возможности сделать антенну малого размера В силу применения радиоэфира для передачи данных, существует большое количество решений для реализации различных атак, как специализированных, типа ProxMark3, так и универсальных, типа HackRF. Два основных вида атак, Relay и Replay, имеют одно общее ограничение: сигнал от метки передается или генерируется устройством нарушителя в силу того, что метка находится вне зоны действия терминала. Программные методы защиты фокусируются на передаче информации, которую нарушитель может перехватить, но не сможет применить повторно, как-то ранее переданное случайное число или ключ сессии. Данные средства защиты частично обходятся методами атак по побочным каналам или уязвимостями, заложенными производителями.

Предлагается следующее средство защиты меток: антенна метки меняется на печатную щелевую антенну со случайным расположением и размерами щелей, получаемых травлением или фрезеровкой, за счет чего каждая метка будет иметь уникальную диаграмму напряженности магнитного поля. Так как щель функционирует подобно диполю, изменением их размеров и местонахождения на покрытии возможно получить значительное количество различных паттернов, с разной

энтропией, градиентом и коэффициентом отражения. В силу большей рабочей зоны UHF меток, позволяющей использовать для идентификации коэффициент отражения, и меньшей длины волны, увеличивающей влияние строения антенны на диаграмму направленности, рекомендуется использовать идентификаторы UHF диапазона.

В силу работы в ближней зоне (< 5 см) предполагается измерение плотности магнитного поля, так как диаграмма направленности имеет значимую роль лишь в дальней зоне. Терминал оснащается антенной решеткой, позволяющей измерить плотность магнитного поля в разных точках пространства и вспомогательным контроллером, рассчитывающим градиент и коэффициент отражения для несущей частоты. Данные значения передаются основному контроллеру, для ускорения процесса возможно привязать данные значения к ключу шифрования некоторой функцией, уникальной для каждой метки.

$$G_u = \frac{1}{M}\sum_{i=1}^{M}\frac{|U_i - U_j|}{d_{ij}}, \quad (1)$$

где G_u – градиент; M – число элементов; U – напряжение; d_{ij} – расстояние между элементами

$$|Ku| = \frac{U_{отр}/U_{вых}}{e^{j\Delta\varphi}}, \quad (2)$$

где $|Ku|$ – модуль коэффициента отражения; $U_{отр}$ – принятое U несущщей (с поправкой на АЧХ антенны и затухание); $U_{вых}$ – U несущей на выходе терминала; $e^{j\Delta\varphi}$ – волновой коэффициент по $\Delta\varphi$

$$\Delta\varphi = -f\frac{d\phi}{df}, \quad (3)$$

где ϕ – мгновенная фаза; f – несущая частота.

Расчеты проводились в САПР Matlab, на базе которого возможно создать приложение, рассчитывающее некоторое количество чертежей антенн с достаточной уникальностью для однозначной идентификации метки.

Для обхода данной методики защиты помимо длительного контакта с меткой, что уже отпугнет большую часть нарушителей, потребуется наличие оборудования, способного измерить характеристики антенны, ПО для расчета 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.

Заключение

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

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

References

1. V. Muravyev, A. A. Tamelo, D. F. Molodkin, D. B. Vladimirov (2010) Calculation and production of antennas and microwave devices. – Minsk, BSUIR.

2. Tanenbaum A. The evolution of RFID security//IEEE Security & privacy. – 2006. – Vol.4, No. 2. – P. 62-69.

Сведения об авторе

Ворожцов А.О. Студент кафедры защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», amdreyvorog2007@gmail.com.

Information about the author

Varazhtsou A., student of Department of Information Security, Educational Institution "Belarusian State University of Informatics and Radioelectronics" amdreyvorog2007@gmail.com.