УЯЗВИМОСТИ ИДЕНТИФИКАТОРА RFID-МЕТОК

С.Н. Петров[1], К.С. Булавин[2], А.О. Ворожцов[2]

[1] *Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь*

[2] *Учреждение образования «Национальный детский технопарк», Минск, Беларусь*

Широкая область применения RFID-систем (систем радиочастотной идентификации) определяет необходимость защиты таких систем, и в особенности, RFID-меток (уникальных идентификаторах), как наиболее уязвимых элементов систем. Разработка механизмов защиты от атак на идентификатор метки способствует безопасному использованию систем на базе RFID в СКУД, здравоохранении, медицине и логистике

Устройство RFID-систем можно разделить на различные уровни, распределенные стандартами и физическими характеристиками меток. Каждый уровень имеет свои уязвимые места, в связи с чем существует большое количество атак на каждый из существующий уровней. Недостаточный уровень защищенности меток на физическом уровне, к примеру, позволяет нарушителю заменить в магазине метку желаемого товара меткой более дешевого товара. Открытость радиоканала, используемого как передачи данных, делает возможным перехват необходимых данных клонирования подлинной метки. На другом уровне нарушитель может использовать пространство метки, выделенное для данных для записи вредоносного кода с целью его дальнейшего распространения.

Эффективная защита RFID-меток достигается добавлением методов противодействия атакам для каждого из уровней коммуникации. Механизм взаимной аунтефикации карты и терминала может предотвратить изменение битов доступа к секторам памяти и перезаписи данных. Данное средство защиты позволяет закрыть возможность считывания данных с карты, выдав устройство за легитимный терминал, в том числе это реализуемо экранированием при помощи материалов, исключающих прохождение какого-либо сигнала. Наличие перезаписываемой памяти позволяет хранить в ней временные метки соединения, за счет которых возможна реализация как взаимной аутентификации, так и использование их для шифрования, как противодействие восстановлению ключа шифрования с последующей расшифровкой. Важной контрмерой является постоянная проверка метки на наличие вредоносного кода во время каждого цикла считывания информации.