DOI: 10.25728/iccss.2022.86.51.036

Зорин В.А., Ненашева Ю.А.

Анализ уязвимостей RFID-меток СКУД на объектах КИИ

Аннотация: Рассмотрены уязвимости RFID-меток, используемые в системах контроля и управления доступом. Приведены предложения для снижения возможности успешных атак.

Ключевые слова: RFID, анализ уязвимостей, объекты КИИ, СКУД

Рост цен на микросхемы и чипы иностранного производства влечёт за собой рост стоимости систем контроля и управления доступом (СКУД). Организации стремятся снизить затраты на инфраструктуру, в связи с чем ищут наиболее доступные решения, закрывающие основные потребности. На объектах критической информационной инфраструктуры (КИИ) ситуация аналогична, поскольку существующие регламентирующие документы [1, 2] не категорируют СКУД. В большинстве случаев СКУД рассматривается как самостоятельный блок, отделённый от производственных процессов.

Целью настоящей работы является рассмотрение уязвимостей RFID-меток, используемых в системах контроля и управления доступом, и атак на них (рисунок 1).

В качестве реализации угроз рассмотрены модели атак на RFID-метку. В работе [3] представлена модель с определением типов и уровней атакующего киберфизическую систему на примере СКУД. Однако приведённая типология не удовлетворяет поставленной в работе задаче, и для этих целей введён дополнительный тип атакующего: «Тип 5. Наличие у атакующего доступа к RFID-меткам, без доступа к системе СКУД. (С применением методов социальной инженерии)».

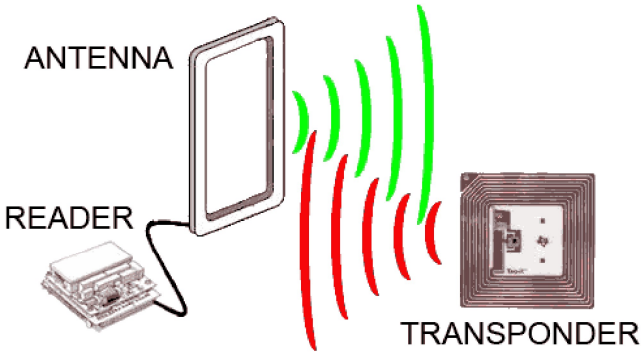

Рисунок 1 – Пример обмена данными RFID-меток в СКУД

Уровень атакующего по модели [3] определён от 1 до 3. Из которых наибольший интерес представляет уровень 2: «Наличие у атакующего специальных знаний о блоках или сети СКУД. Атакующий может использовать специализированные инструменты и эксплуатировать уязвимости нулевого дня (примеры атакующих действий: атаки типа «человек-посередине», отказ в обслуживании, переполнение буфера)».

Существующие уязвимости использования карт доступа.

1. Незащищенность данных. UID хранится в открытом виде и не защищён от считывания, что делает карту доступа и всю систему уязвимой, позволяя злоумышленникам получить не только доступ к объекту, но и информацию о владельце карты. Проблема частично решается применением алгоритмов шифрования. Стандартизированные Международной организацией по стандартизации (ISO) в рамках стандарта радиоинтерфейса RFID-шифры по состоянию на октябрь 2018 г. были успешно подвергнуты криптоанализу [4] с использованием метода Раддума-Семаева.

2. Повторное воспроизведение. При каждом чтении карты передается одна и та же информация, которую можно перехватить, записать и повторно воспроизвести для получения доступа. Защитой от повторного воспроизведения служит взаимная аутентификация карты доступа и считывателя.

Рассмотрен частный случай атаки на RFID-метку с целью компрометации уникального идентификационного номера (UID), в бесконтактных картах доступа ISO 14443, по типу Mifare, каждая RFID-метка Mifare оснащена UID и памятью с возможностью перезаписи. UID не является секретным и не подлежит защите,

соответственно не относится к зашифрованной информации. Считывание данных из карты памяти и запись информации на нее осуществляется исключительно при наличии специальных кодов доступа. Данные, которые передаются между ключом и считывателем, зашифрованы. Считыватели одновременно распознают как UID, так и информацию, расположенную в зашифрованной памяти. Наиболее распространенные системы контроля и управления доступом не обладают такой возможностью и считывают только UID. Системы СКУД, которые поддерживают работу с двумя способами идентификации одновременно – с памятью и UID стоят дороже и на практике встречаются редко.

Для атаки на RFID-метку используется дубликатор, например, SMKey [5], позволяющий получить криптоключ для чтения Mifare непосредственно от самого считывателя, что дает возможность изготовить копию метки даже со всеми закрытыми секторами (рисунок 2). Дубликатор имеет память на 18 ячеек (ключей). Скопированный UID в дальнейшем записывается на заготовки MF Zero и MF OTP, либо используется дубликатором в режиме эмуляции для получения несанкционированного доступа.

Рисунок 2 – Пример дубликатора RFID-меток

Способы защиты от атак.

1. Взаимная аутентификация. При наличии алгоритма взаимной аутентификации, карта доступа, попадая в зону считывания, предоставляет считывателю свой уникальный номер CSN и

сгенерированный 16-битный случайный номер. В ответ считыватель, используя Hash-алгоритм, создает диверсификационный ключ, который должен совпасть с ключом, записанным на карте. При совпадении – карта и считыватель обмениваются 32-битными откликами, после чего считыватель «принимает» решение о валидности карты. Таким образом, осуществляется защита от повторного воспроизведения информации. Однако в большинстве систем взаимная аутентификация не используется.

2. Диверсификация ключа. С помощью программного обеспечения настраивается разграничение доступа для повышения надежности СКУД на следующих уровнях:

А) «Дверь» – доступ в помещения разграничен в соответствии со служебными обязанностями и полномочиями. Однако, данный способ не защитит, в случае компрометации карты сотрудника, имеющего повышенный уровень доступа;

Б) «Время» – после окончания рабочего дня, а также в выходные и праздничные дни доступ может быть ограничен;

В) «Запрет повторного прохода» – разграничение запрещает проход злоумышленника с клоном карты присутствующего на рабочем месте сотрудника, а также запрещает работникам пропускать по своей карте посторонних.

В работе [6] отмечается актуальность и перспективность использования комбинированных СКУД в задачах цифровизации, однако критериев рациональности использования таких систем в условиях высокой стоимости комплектующих не приведено.

В результате анализа уязвимостей RFID-меток в системе контроля и управления доступом на объектах критической информационной инфраструктуры следует учесть возможность компрометации карт доступа, использующих RFID. Предусмотреть комбинированный способ разграничения доступа и одновременное считывание данных UID и информации в зашифрованной области памяти RDIF-меток.

Литература:

1. Федеральный закон от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

2. Постановление Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

3. *Левшун Д.С., Чечулин А.А., Котенко И.В.* Комплексная модель защищенных киберфизических систем для их проектирования и верификации // Труды учебных заведений связи. – 2019. – Т. 5. № 4. – С. 114-123.

4. *Куценко А.В., Атутова Н.Д., Зюбина Д.А., Маро Е.А., Филиппов С.Д.* «Алгебраический криптоанализ низкоресурсных шифров Simon и Speck» // ПДМ. Приложение. – 2021. – № 14. – С. 84-91.

5. iKey – Всё для копирования ключей [Электронный ресурс]. – URL: https://ikey.ru/smkey/ (дата обращения 14.10.2022).

6. *Горохов А.В., Гаврин В.А., Мартынов В.А.* Обеспечение информационной безопасности посредством построения комбинированных систем контроля и управления доступом // Научно-образовательный журнал для студентов и преподавателей «StudNet». – 2022. – Т.5. №4. – Порядковый номер: 26.

DOI: 10.25728/iccss.2022.61.81.037

Логинова Л.Н., Королев А.Д.

Принципы обеспечения информационной безопасности в социальных сетях

Аннотация: В работе показаны особенности обеспечения информационной безопасности в социальных сетях, проведен анализ существующих способов защиты, даны рекомендации по защите информации и персональных данных.

Ключевые слова: информационная безопасность, утечка данных, защита информации, социальные сети, аутентификация