Роль СКУД в обеспечении защиты несанкционированного доступа в служебные зоны отеля

Николай Желтов,

директор по продукту ESMART®, отвечает на часто задаваемые вопросы по оснащению и закупкам оборудования СКУД для объектов гостиничной, санаторной и курортной инфраструктуры.

Вопрос: Какие новинки для СКУД, в частности для отелей и туристической инфраструктуры, вы можете предложить на сегодня?

Н.Ж.: Подход к внедрению СКУД за последние 5 лет претерпел множество изменений. Сегодня в тренде интегрированные системы контроля и управления доступом. Такие системы работают совместно с видеонаблюдением, видеоаналитикой, системами учета рабочего времени, доступа в номера, управлением бронированием номеров, телефонией и прочими системами, без которых современные отели не могут обойтись. Безопасность, обеспечиваемая СКУД в гостиницах и отелях, – это первый рубеж предотвращения краж из номеров, защиты от несанкционированного доступа в служебные зоны и терроризма. В то же время становятся актуальными вопросы комфортности систем безопасности для сотрудников и гостей – они не должны ощущать на себе постоянную слежку и волноваться за конфиденциальность своих данных, при этом системой СКУД должно быть удобно пользоваться.

Наша компания уже 20 лет занимается решениями в области информационной безопасности и СКУД. Мы оценили запросы рынка, как со стороны экспертов в вопросах безопасности, так и со стороны пользователей, и разработали современное решение для СКУД под брендом ESMART® Доступ. Оно объединяет высокий уровень безопасности и защиты СКУД отеля от внешних и внутренних угроз с удобством и простотой использования для гостей и обслуживающего персонала.

Решение включает в себя широкую линейку считывателей ESMART® Reader в разных дизайнах и формфакторах, физические и виртуальные идентификаторы ESMART® Доступ для прохода, и мобильное приложение ESMART® Конфигуратор, которое позволяет администраторам настроить требуемые параметры работы системы.

Вопрос: От каких угроз позволит защитить отель ваше решение?

Н.Ж.: На сегодняшний день в системах контроля и управления доступом можно выделить следующие наиболее распространенные виды угроз:

- Копирование идентификатора пользователя на сторонние носители, фактически использование неоригинальной копии смарт-карты.
- Подслушивание идентификатора пользователя СКУД в одном из двух каналов передачи (карта – считыватель, считыватель – контроллер) с целью его воспроизведения, опять же, на стороннем носителе, даже на оригинальном.
- Передача карты пользователя в сторонние руки как умышленно, так и неосознанно.
- Саботаж от самих сотрудников отеля с целью определенной выгоды.

ВЕРНУТЬСЯ К СОДЕРЖАНИЮ

Давайте разбираться по порядку.

Одной из самых распространенных проблем в большинстве систем контроля доступа является использование карт, работающих на устаревших технологиях. Об этом известно как игрокам рынка, так и продвинутым пользователям, которые используют подобные уязвимости в своих целях.

Например, карту с технологией 125 кГц (форматы Em-Marine, HID Prox, Indala и другие) можно легко клонировать в мастерских по изготовлению ключей и дубликатов, буквально за копейки.

Рынку также давно известно слово MIFARE (на слуху как «Майфер», «Мифар», «Мифаре»). Многие считают использование подобных карт панацей для решения проблемы подделки. Но истина кроется в деталях. MIFARE® – это бренд компании NXP Semiconductors, под которым выпускается целая линейка карточных чипов, ряд из которых действительно безопасен и на момент написания статьи копированию не подлежит (на этом мы подробнее остановимся позже). А вот самый часто используемый формат, так называемый MIFARE® Classic, легко скопировать доступными на рынке средствами из-за уязвимости в алгоритме шифрования Crypto1, который был скомпрометирован еще в 2007 году. Кстати, по нашему опыту, как раз карты MIFARE® Classic чаще всего используют в отелях для доступа в номера.

Наше решение позволяет избежать описанных выше рисков благодаря возможности использования одного из двух безопасных вариантов работы, которые гарантируют возможность использования в СКУД только тех карт, которые были выданы в бюро пропусков или на ресепшене отеля:

1. Использование карт формата MIFARE® Plus в режиме **SL3 (Security Level 3)** с применением шифрования AES128 – оно надежно защищает карту от попытки несанкционированного чтения идентификатора пользователя и переноса его на сторонний носитель. Карты с данной технологией доступны в продаже в большинстве профильных торговых домов на рынке, причем вы сможете заказать данные карты сразу с запрограммированным ключом AES128, если у вас есть оформленное техническое задание на электронную персонализацию карты.
2. «Коробочное решение» для защиты карт от подделки нашей собственной разработки – идентификаторы на базе технологии ESMART® Доступ с 6 степенями защиты от копирования и подделки: шифрование AES128, диверсификация ключей шифрования, CMAC-подпись идентификатора, защита от replay-атак и гарантия уникальности идентификатора. Подобные карты нативно и безопасно работают с любыми считывателями ESMART® Reader и не требуют дополнительной электронной персонализации. Такой вариант удобен тем, что не требует дополнительных действий и оборудования от владельца системы, а также защищает от саботажа самих сотрудников. Такую карту нельзя перевыпустить на стороннем носителе, а доступ в различные зоны отеля определяется только через интерфейс СКУД, где все действия администратора отслеживаются и логируются.

Оба варианта надежно защищают карту от риска изготовления дубликата. При таком подходе исключены риски «подслушивания» команд с помощью специальных устройств (снифферов).

Технологии обсудили, но необходимо упомянуть еще один ключевой факт, я его считаю основополагающим:

> Если на объекте предполагается использование карт разного формата (с разными технологиями безопасности и защиты от копирования) одновременно, то уровень безопасности всей СКУД сводится к уровню безопасности наименее защищенной карты.
>
> Это говорит о том, что какие бы защищенные карты ни применялись на объекте, в случае если наравне с ними считыватели работают с менее защищенными картами – это является прямым риском безопасности, на который стоит обратить пристальное внимание.

В нашем решении мы предусмотрели возможность ограничивать функционал считывателей на чтение строго определенного формата карт, запрещая чтение других форматов. К примеру, если вы приняли решение использовать для прохода в служебные зоны в отеле карту MIFARE® Plus в режиме SL3, – вам следует отключить в настройках считывателя ESMART® Reader чтение всех других форматов карт, таких как MIFARE® Classic, MIFARE® ID, Ultralight и прочих. В этом вам поможет наше бесплатное мобильное приложение ESMART® Конфигуратор. Оно позволяет создать необходимый набор настроек для соответствующей модели считывателя самостоятельно, а затем загрузить их в устройство по Bluetooth, без демонтажа считывателя и обесточивания системы.

Вопрос: Разве современных средств защиты карт недостаточно? Почему нужно ограничивать работу считывателей на определенные виды карт?

Н.Ж.: Мы плавно перешли к следующему виду атак – на уязвимые проводные протоколы передачи данных теперь уже от считывателя к СКУД-контроллеру.

По нашей оценке, подавляющее большинство уже эксплуатируемых СКУД в России использует распространенный стандарт Wiegand. Он не вызывает сложностей при пусконаладке и монтаже системы, а устройства легко взаимозаменяемы благодаря универсальности интерфейса. В ассортименте ESMART® есть считыватели с Wiegand-интерфейсом – линейка ESMART® Reader BLE. Она пользуется большой популярностью, особенно там, где нет возможности замены всей СКУД целиком, но допустима замена только считывателей с подключением к уже установленным СКУД-контроллерам, с целью перехода на более безопасные идентификаторы.

Наряду с озвученными преимуществами есть, конечно, и недостатки – стандарт Wiegand не подразумевает защиту передаваемого номера карты. Номер передается в открытом виде, средства криптографии применить невозможно, так как стандарт подразумевает только одностороннюю передачу данных – от считывателя к контроллеру. Таким образом, злоумышленник может узнать значение идентификатора карты, подслушав его, подключившись к интерфейсу Wiegand, минуя все механизмы защиты самой карты.

Нам известен прецедент, который произошел у одного из крупных застройщиков с использованием такой уязвимости на оборудовании одного из известных брендов считывателей. Считыватель был настроен на чтение всех видов карт без ограничений, а дополнительной настройкой было включено чтение карт MIFARE® Plus в режиме SL3. Пользователям на объекте, безусловно, были выданы безопасные карты MIFARE® Plus в режиме SL3.

Злоумышленник, имея на руках считыватель с объекта и карту сотрудника, получил идентификатор карты, подслушав номер по Wiegand-интерфейсу. Затем записал этот номер на клон карты MIFARE® Classic (широко известный под названием Zero) и получил несанкционированный доступ в СКУД, потому что на считывателе было разрешено чтение всех карт, а не только карт MIFARE® Plus. Насколько нам известно, оборудование бренда просто не позволяет отключить чтение других карт.

Вопрос: Какой вариант защиты вы предлагаете?

Н.Ж.: Избежать подобных инцидентов позволит использование нашей последней линейки устройств – ESMART® Reader PRO. Ключевой особенностью линейки является поддержка нового стандартизированного протокола обмена данными между считывателем и СКУД-контроллером – OSDP (Open Supervised Channel Protocol).

Протокол подразумевает двухстороннюю связь между считывателем и контроллером, что позволяет производить шифрование данных с применением современной криптографии.

Использование OSDP решает поднятую ранее проблему, в случае если и оба устройства, и СКУД-контроллер и считыватель поддерживают так называемый режим шифрования канала – **Secure Channel**. Наши устройства поддерживают этот режим стандарта OSDP из коробки.

Также OSDP дает возможность одновременной удаленной настройки и обновления прошивки для всех считывателей в случае поддержки данной функции со стороны СКУД-контроллера. Это гарантирует работу системы на последних версиях программного обеспечения, снижает затраты на выезд специалистов для обслуживания и повышает уровень контроля за всей системой безопасности.

Для номерного фонда отеля считыватели ESMART® Reader PRO могут работать автономно без контроллера, имея собственную память идентификаторов, этот режим мы называем SOLO. Электронные замки, кнопки выхода и герконы подключаются напрямую к считывателю, управление дверью происходит благодаря встроенному реле. Мы предусмотрели возможность гибкой настройки устройства для поддержки работы с разными типами замков. Это позволяет соблюдать требования к противопожарной или антитеррористической защищенности, предъявляемые для туристических объектов.

Вопрос: Один из самых болезненных вопросов к карточным СКУД – передача карт в чужие руки. Как это решить?

Н.Ж.: Не секрет, что классические карты доступа, которые обычно выдают гостям в качестве ключей, совсем не защищены от безответственного отношения. Их теряют, ломают, а при худшем сценарии умышленно передают посторонним. Главный корень проблемы – низкий уровень личной заинтересованности пользователя в сохранности карты. Ценность такого носителя очень маленькая, к тому же карту

неудобно всегда держать «под рукой» – в кармане или кошельке. Другое дело – телефон.

Сегодня невозможно представить жизнь современного человека без мобильного телефона: в нем заключены все рабочие процессы и личная жизнь. Мобильный тренд прочно вошел в нашу жизнь – безусловно мы не могли обойти его стороной. Приложение ESMART® Доступ заменяет физическую карту – виртуальной. Мобильный доступ работает благодаря технологиям Bluetooth и NFC, которые поддерживаются нашими считывателями. Приложение доступно для операционных систем iOS и Android. Мы позаботились о вашей безопасности, внедрив в приложение нашу технологию безопасности ESMART® Доступ, и защитили виртуальную карту от копирования или переноса в другие телефоны.

Пользователю доступны два режима использования. В режиме «Прислони как карту» пользователь прислоняет телефон к считывателю вплотную, аналогично привычному опыту использования физической смарт-карты. Либо выбирает совершенно новый пользовательский опыт в режиме «Свободные руки», когда телефон лежит в кармане и для прохода достаточно просто подойти к двери. В этом случае дальность срабатывания для каждой конкретной точки прохода может ограничить администратор СКУД с помощью мобильного приложения ESMART® Конфигуратор.

По нашей оценке, для отелей и гостиниц с 3–4-й категорией опасности такое решение необходимо и достаточно для закрытия вопросов безопасности на высоком уровне.

Для объектов с самыми высокими категориями опасности мы рекомендуем использовать дополнительные факторы наравне с мобильным доступом. Двухфакторная аутентификация в СКУД обеспечит максимальный уровень защиты как от краж, так и террористических угроз.

Вопрос: Что еще полезного предлагаете для отелей в решении СКУД?

Н.Ж.: Мы предусмотрели возможность заказа наших устройств с индивидуальным дизайном от одной штуки. Клиент может выбрать цвета корпуса, текстуру и нанесение любой графики, логотипов, текстов и фирменных элементов.

По нашей оценке, отельеры очень щепетильно относятся к созданию стильной и гостеприимной атмосферы в своих заведениях, поэтому считыватели ESMART® – идеальный выбор для объектов туризма. По желанию клиента они могут быть незаметными в интерьере или наоборот – являться ярким акцентом, помогая строить сильный туристический бренд. Также мы рекомендуем использовать возможности дизайна считывателей для навигации на объекте, как один из ярких примеров – обозначить staff-зоны для сотрудников и помогать с нумерацией комнат и помещений.

Вопрос: В связи с нестабильной геополитической ситуацией влияют ли на ваши решения санкционные ограничения?

Н.Ж.: Нет. У нас полный цикл разработки и собственное серийное производство в России, мы используем ПО собственной разработки, которое развернуто на собственных серверах. Мы не применяем облачные продукты, с проблемой отключения которых сейчас массово сталкиваются российские пользователи. Тем не менее мы отмечаем очевидный рост цен на комплектующие и контролируемое увеличение сроков их поставки из-за изменений логистических путей.

ПОДРОБНЕЕ О РЕШЕНИЯХ СКУД для объектов гостиничной, санаторной и курортной инфраструктуры >>>

На этой странице текст зеленого цвета содержит гиперссылку