Безопасность СКУД:
технологии идентификации и форматы карт

Владимир НАРОЖНЫЙ,
эксперт

Юрий КОНДРАТЬЕВ,
менеджер по системам безопасности TerraLink

Одним из ключевых критериев оценки СКУД является безопасность на всех уровнях цепочки идентификатор – считыватель – контроллер – сервер – удаленное рабочее место. В данной статье мы рассмотрим наиболее актуальный вопрос – безопасность передачи данных от идентификатора к считывателю.

ИДЕНТИФИКАТОРЫ КАК ЧАСТЬ НАШЕЙ ЖИЗНИ

Сложно представить современный мир без контактных и бесконтактных технологий идентификации. Использование банковских карт (с магнитной полосой, карты с чипом EMV, бесконтактные платежи PayPass, payWave); RFID-карты для транспорта, сферы развлечений и программ лояльности: выдача полисов ОМС и социальных карт москвича и, конечно же, карты физического доступа и логического доступа к компьютеру и ИТ-ресурсам компании – наиболее яркие примеры повсеместного применения идентификаторов.

СУЩЕСТВУЮЩИЕ ТЕХНОЛОГИИ НА УЧАСТКЕ КОММУНИКАЦИЙ МЕЖДУ СЧИТЫВАТЕЛЕМ И КАРТОЙ

Если взглянуть на историю развития систем контроля доступа, мы увидим, что первые из них, использующие электронно-вычислительную технику, были применены еще в конце XIX века в виде электрических табулирующих систем Hollerith technology, в которых вместо современных считывателей и карт использовались табуляторы и перфокарты. На сегодняшний день благодаря естественному прогрессу на смену огромным машинам (табуляторам) и картону (перфокарта) пришли компактные высокотехнологичные устройства.

Основные технологии:
- Штрих-код
- Магнитная полоса
- Wiegand-карта
- EM Marine (125 КГц)
- Prox (производитель HID Global, 125 КГц)
- Legic (производитель Legic, 1992 год)
- Mifare (производитель Philips, 1994 год)
- Mifare DESFire (производитель Philips, 2006 год, 13,56 МГц)
- iCLASS SE (производитель HID Global, 2012 год, 13,56 МГц)

Остановимся на более распространенных радиочастотных технологиях с частотой 125 КГц (EM Marine, HID Prox, Indala) и 13,56 МГц (Mifare DESFire, iCLASS SE)

УЯЗВИМОСТЬ ТЕХНОЛОГИЙ СЧИТЫВАНИЯ

В первую очередь определимся с тем, что карта – это идентификатор пользователя, на котором содержится некая информация – ключ, открывающий дверь или доступ к ресурсам. Именно поэтому вопрос безопасности передачи данных от идентификатора к считывателю, как никогда, актуален. Степень риска копирования информации с карт и их клонирования увеличивается ежедневно, и это заставляет более осознанно подходить к выбору технологий, обеспечивающих безопасную идентификацию.

Как правило, уязвимость оценивают по трем основным угрозам, выявленным в процессе эксплуатации бесконтактных карт: повторное воспроизведение, клонирование и конфиденциальность данных. См. таб. 1.

Исходя из таблицы, можно сделать вывод, что среди всех радиочастотных технологий карты 125 кГц наиболее уязвимы с точки зрения уровня безопасности в связи с возможностями:
- повторного воспроизведения, так как при каждом чтении карты передается одна и та же информация, которую можно перехватить, записать и воспроизвести для получения доступа в помещение;
- клонирования программатором незаметно для владельца карты;
- незащищенности конфиденциальных данных – идентификатор хранится в открытом виде и никак не защищен от считывания.

Рассмотрим основные способы защиты от угроз, заложенные в алгоритм работы смарт-карт. Обратная связь между устройствами является ключевым вопросом обеспечения безопасной идентификации в цепочке карта – считыватель.

Таблица 1

	Угроза безопасности			
	Повторное воспроизведение	Клонирование	Конфиденциальность данных	Дополнительный уровень безопасности
	Защита от угроз			
	Взаимная аутентификация	Диверсификация ключа	Шифрование DES, 3DES, AES	Привязка к UID/CSN, CMAC 96
Технология RFID				
EM Marine	Нет	Нет	Нет	Нет
Mifare	Да, но открытая	Нет	Нет	Нет
DESFire EV1	Да	Да	Да	Нет данных
iCLASS SE	Да	Да	Да	Да

Карта, попадая в зону считывания, предоставляет ридеру 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, защита карт 13,56 МГц от обозначенных выше угроз обеспечивается за счет взаимной аутентификации между картой и считывателем, процесс которой происходит в зашифрованном виде с формированием и подтверждением ключа диверсификации.

Однако идентификатор сегодня – это больше, чем пропуск в помещение. Сегодня все чаще используется единый идентификатор, который обеспечивает доступ как в здание и служебные помещения, так и к корпоративной информации и управлению ИТ-средой. Это требует от производителя карт дополнительных мер для обеспечения безопасной идентификации.

Среди них следует выделить технологию Secure Identity Object™ (SIO), которая обеспечивает многоуровневую защиту данных и представляет собой электронный контейнер для хранения данных в любом из форматов карт.

Вкратце о технологии: во время кодирования карты происходит привязка к уникальному идентификатору носителя UID с последующим заверением записанной информации электронной подписью. Присвоение UID и наличие электронной подписи исключают возможность копирования информации и взлома защиты карты.

ОПРЕДЕЛЯЕМСЯ С ФОРМАТОМ КАРТ

Формат бесконтактной карты доступа определяет количество бит и способ их комбинирования, к примеру, карта формата EM4100 (EM Marine) работает на частоте 125 кГц и содержит уникальный номер длиной в 40 бит, который присваивается в дальнейшем пользователю.

Все старательно избегают этого вопроса, хотя ответ на него имеет первостепенную важность при выборе и программировании любых средств доступа.

Немаловажным критерием безопасности карт как носителей информации является культура их производства, отношение владельца технологии к организации процесса выпуска.

В отличие от EM4100 представленные на рынке смарт-карты могут содержать несколько областей памяти, серийный номер CSN, номер и серию (или фасилити код), а также другую служебную информацию. Так, корпорация HID Global предлагает различные форматы карт, на каждом из которых могут содержаться различные технологии безопасности. См. таб. 2.

Выбор формата имеет серьезное значение как для работы системы, так и для ее безопасности. Что такое формат?

Формат – это структура данных, хранящихся в памяти средства доступа. По своей сути это набор двоичных цифр (бит), в определенном порядке образующих двоичное число, которое система контроля преобразует в код доступа. Количество единиц и нулей и способ их комбинирования определяют формат, в котором зашифрован код доступа.

Так, 26-битный открытый формат H10301 допускает 255 кодов объекта (фасилити кодов), в каждом из которых возможны 65 535 комбинаций номеров карт. При этом производитель не контролирует и не ограничивает производство карт данного формата, что увеличивает риск их дублирования.

В отличие от формата H10301 формат H10304 имеет 37-битную длину кода и позволяет задавать 65 535 кодов объектов и более 500 000 номеров карт для каждого кода объекта, что существенно увеличивает диапазон карт. Помимо этого производитель отслеживает производство этих карт.

Формат Corporate 1000 представляет собой 35-битный формат, разработанный как собственный закрытый формат для крупных компаний.

Таким образом, при выборе технологии идентификации для организации системы СКУД рекомендуем обратить внимание на форматы карт. Выбор и использование того или иного формата также оказывает влияние на общий уровень безопасности системы.

Таблица 2

Технология RFID	Формат			
	H10301	H10302	H10304	Corporate 1000
Prox	√	√	√	√
Indala	√	√	√	√
iCLASS	√	√	√	√
iCLASS SE	√	√	√	√
SeoS	√	√	√	√

ПРЕЕМСТВЕННОСТЬ И СОВМЕСТИМОСТЬ ТЕХНОЛОГИЙ

Под преемственностью технологий принято понимать поддержку со стороны производителя ранее выпущенных продуктов и возможность работы старых и новых технологий в рамках одной системы.

Все преимущества преемственности технологий проявляются во время модернизации или масштабирования точек доступа или функционала системы. При этом в рамках СКУД стоит рассматривать преемственность как со стороны аппаратной части (поддержка или перепрошивка считывателей и контроллеров, одновременное использование карт), так и программного обеспечения.

Как правило, в процессе модернизации или расширения систем контроля доступа применима одна из схем: полная или частичная замена оборудования, полная или частичная замена программной части. При частичной замене оборудования, как правило, используют мультиформатные (комбинированные считыватели) и/или мультиформатные карты доступа. Таким образом, преемственность технологий обеспечивает оптимальный способ последующего апгрейда системы без полной замены аппаратной части системы.

Совместимость технологий разных производителей позволяет использовать различные технологии и форматы идентификаторов в рамках одной системы. Как правило, это оптимальное решение для объектов, на которых уже используются определенные технологии, функционирует система, и процесс миграции на новые технологии осуществляется поэтапно без остановки процессов на предприятии.

РЕЗЮМЕ

Идентификаторы в системе в СКУД сегодня – это больше чем «таблетки» Touch Memory и proximity карты. Вопрос защищенности технологий идентификации не менее актуален, чем анализ и оценка функционала и возможностей системы на уровне ПО.

Помимо традиционных способов защиты карт – взаимной аутентификации устройств, шифрования данных и использования ключей диверсификации – на рынке представлены решения, обеспечивающие дополнительный уровень безопасности при передаче данных от идентификатора к считывателю. Одно из решений – платформа SIO, получившая распространение в устройствах iClass SE.

Дополнительным критерием выбора технологии идентификации является формат карты. Отдельным вопросом является защищенность формата производителем, а также культура производства карт.

Преемственность технологий, которую обеспечивает производитель в процессе эволюции своих решений, и совместимость технологий разных производителей, которую можно организовать в рамках одной системы, – это концептуальные вещи, которые необходимо учитывать как при выборе и монтаже системы СКУД с нуля, так и для организации процессов модернизации действующих систем контроля доступа, их расширения и встраивания в бизнес-процессы компании.