КОЛОНКА РЕДАКТОРА

Этот народ непобедим!..

Уверен, что большинство коллег, успевших пожить в СССР, помнят бородатый анекдот про суровых сибирских мужиков, которым на пилораму в тайге привезли японскую пилу... и ею попробовали в конце истории распилить лом.

Я не случайно вспомнил эту байку – она неизменно возникала у меня в памяти в процессе чтения статьи Алексея Омельянчука "Алгоритмы повышенной защиты доступа и способы народной борьбы с ними", как и слова нашего записного юмориста Задорнова: "Этот народ нельзя победить!.."

На любую хитроумную "гайку" наши отечественные Кулибины очень быстро находят подходящий "болт". Эта статья будет весьма полезна прежде всего администраторам – тем специалистам, которые занимаются эксплуатацией систем контроля и управления доступом на объектах.

Наши пользователи научились обходить не только бабушек-вахтеров, но и современные электронные средства, поэтому сотрудникам служб безопасности и компаниям, специализирующимся на внедрении СКУД, будет нелишним знать о типовых (и не очень типовых) уловках пользователей.

Другой материал этого номера – статья Алексея Юрченко "Как удешевить проект СКУД?" – направлен также на потребительскую аудиторию. Вопрос оптимизации затрат при внедрении новых систем обычно один из самых актуальных для заказчика.

Для таких сложных систем, как СКУД, количество исходных параметров чрезвычайно велико, и зачастую потребителю из огромной массы данных трудно выделить самые главные. Критерии стоимости обычно входят в первую тройку наиболее важных, и Алексей предлагает в процессе оценки разных систем использовать такой экономический показатель, как совокупная стоимость владения системой – понятие, которым широко оперируют поставщики и потребители на Западе.

Уважаемые читатели, приглашаю вас присылать ваши предложения по новым и интересным темам для обсуждения в редакцию. Традиционно наиболее интересные и животрепещущие темы попадают в редакционный план – в интересах пользователей и поставщиков оборудования и услуг безопасности.

Алексей Гинце
Редактор раздела "Системы контроля и управления доступом"

Алгоритмы повышенной защиты доступа

и способы народной борьбы с ними

Современные системы контроля доступа пока не привнесли ничего нового в собственно алгоритмы ограничения доступа. Просто раньше эти алгоритмы обеспечивались механическими устройствами, а чаще – организационными мерами. Теперь за соблюдением "установленного порядка" следит электроника

Алексей Омельянчук
Начальник КБ
компании "Сигма-ИС"

Конечно, за счет автоматизации применение усиленных алгоритмов стало более удобным и более распространенным. А поскольку для нарушения инструкции теперь недостаточно общего разгильдяйства, вырабатываются специфические способы обмана электронной системы – ведь люди по-прежнему понимают необходимость строгих мер защиты, но также по-прежнему не понимают, почему именно они обязаны им следовать и тратить свое драгоценное личное время на выполнение придуманных кем-то инструкций.

Все многообразие специальных, усиленных алгоритмов доступа можно разделить на несколько основных классов.

Класс первый – принцип комиссионности

Это главный класс. Во многих случаях в ныне действующих инструкциях, как и много лет назад, требуется, чтобы определенные действия осуществлялись обязательно не одним человеком, а несколькими – "комиссией". Например, снимать кассу, открывать помещение сортировки алмазов, оружейную комнату и т.д. можно только вдвоем (или втроем), причем один должен быть, скажем, дежурным офицером охраны, второй человек – старшим инженером смены, а третий, условно говоря, представителем от профсоюза.

Современные электронные системы реализуют такой подход в виде нескольких схожих алгоритмов. Все они требуют предъявить несколько документов, принадлежащих разным лицам примерно в одном месте. Предельный случай защищенности – когда на расстоянии нескольких метров установлено несколько считывателей отпечатков пальцев (или сканеров сетчатки глаза), которые должны сработать одновременно с точностью около секунды. Такая система весьма дорога, но обмануть ее в рамках нормального функционирования почти невозможно.

Однако собираться втроем, отрывать занятых людей каждый раз, когда надо всего лишь поменять перегоревшую лампочку в этой комнате, очень утомительно.

В практике известны различные способы преодоления алгоритма, которые базируются в основном на такой идее: один раз инструкцию выполним, а потом будем ходить по более простому варианту.

Например, после вскрытия помещения замок механически блокируется, чтобы дверь не захлопнулась, и весь день помещение стоит открытым, даже когда все ушли на обед. Если вместо считывателей пальцев применяются обычные считыватели Proximity-карт (часто вообще один, на котором надо поочередно предъявить несколько карт), то обычно дело кончается тем, что карта "дежурного офицера" просто лежит рядом со считывателем, и любой желающий подносит свою карту, лежащую рядом карту "офицера" и проходит один, без всякой комиссии. Ну а "офицер", поскольку без карты он не может перемещаться по объекту, с чистой совестью спит всю смену в комнате отдыха.

Бороться с таким сговором очень трудно, помогают только биометрические считыватели – вряд ли даже самый ленивый офицер согласится оставить перед секретной комнатой свой глаз или палец

Класс второй – просто повышенный контроль

Под усиленными алгоритмами второго класса подразумевается контроль нескольких параметров. Помните, в старорежимные времена для прохода в особо секретный корпус в НИИ типа "почтовый ящик" требовалось не только предъявить пропуск, но еще и назвать секретный номер, по которому вахтер найдет у себя в ячейке не подлежащий выносу пропуск с фотографией, сравнит ее с вашим невыспавшимся

лицом, да еще и проверит, есть ли ваша фамилия в списке на сегодня.

Сейчас это обеспечивается установкой нескольких считывателей разного типа, в простейшем варианте – считыватель карты и клавиатура набора кода, что позволяет не пустить карманника, вытащившего у вас пропуск в трамвае по дороге на работу.

Многие не очень честные люди норовят давать свои карточки кому-то другому, чтобы тот отметился за них на входе с утра пораньше (учет рабочего времени обмануть) или, наоборот, чтобы молодого, кому в рабочее время не положено, послать в буфет за баранками.

В общем, многие передают свою карточку в пользование другим людям, для чего записывают на ней свой секретный персональный код.

Защитой от этого может быть опять же только биометрический считыватель

Причем популярные на некоторых объектах псевдобиометричекие "весы" не помогают. Довольно легко подобрать нужное усилие, с которым надо чуть подтянуться на прутьях турникета, чтобы сымитировать вес худенькой девушки. Или наоборот. Второй вариант обмана – пройти самому, честно предъявив и карту, и ПИН-код, и сетчатку глаза, после чего пропустить в дверь еще нескольких человек. Даже турникеты не вполне спасают.

Третий класс – логический контроль

К данному классу относятся алгоритмы повышенной защиты, исключающие повторный проход. Например, зональный или временной антипассбэк. Во времена механических ячеек с пропусками это было само собой разумеющимся. Пройти второй раз по одному пропуску можно, только когда вахтер снова положит его в ячейку. Даже если вы сразу кинете пропуск, будто сдали его на выходе, обратно в ячейку его положат лишь после "часа пик", когда вахтер разогнет спину, пропустив тысячу человек на смену.

Электроника работает более изощренно – она может требовать, чтобы данная карта не применялась для прохода в течение какого-то времени здесь или на удаленных отсюда считывателях. Или наоборот, чтобы предыдущий раз она была предъявлена именно на входе в помещение, из которого вы теперь пытаетесь пройти дальше.

Как побочный бонус: электронные системы могут считывать, сколько человек находится в помещении. Тут алгоритм смыкается с "комиссионностью" или, напротив, реализует защиту от переполнения – например, число людей в комнате для работы с секретными документами не должно превышать количество мест.

Увы, обмануть такую систему не так уж и трудно, хотя порой утомительно. Один человек с пачкой карточек может заставить систему "думать", что все 40 человек находятся на службе, когда они на лавочке во дворе на солнышке греются.

Защитить систему можно только установкой многочисленных шлюзов или турникетов, затрудняющих повторное предъявление новой карты тем же человеком (или той же карты другим человеком)

Шлюз как особая категория

Шлюз можно также считать особой категорией алгоритмов усиленного доступа, ведь это именно алгоритм работы двух дверей, при котором они открываются поочередно. Конечно, есть и аппаратные (механические) реализации шлюза, вроде поворотного цилиндра, который в принципе не может быть открытым с обеих сторон одновременно. По эффекту шлюз вполне можно сравнить с турникетом.

Главное свойство обоих устройств – способность пропускать людей строго по одному. Однако в этом нельзя быть вполне уверенными.

Анекдот из жизни № 1

Я сам, в свое время неосторожно прокрутив на лишний оборот турникет, оказался перед запертым шлюзом (да-да, шлюз был организован из двух турникетов. Система считала, что я уже внутри и отказывалась пропускать повторно. Начальник охраны алмазной шахты в ЮАР (да-да, лично!) сказал, что ему лень звонить на центральный пост, чтобы меня разблокировали, позвал самого худенького из стоявших рядом негров, дескать, вы и вдвоем протиснетесь. Действительно, если через турникет может пройти один толстый, то два (или даже три) тонких там тоже пройдут.

Анекдот из жизни № 2

Бывает и другое. Шлюз, электроника разрешает открывать двери строго поочередно, внутри биометрический считыватель. Солдатам срочной службы понадобился всего месяц, чтобы найти слабое место системы – если поднести карту с одной стороны, потом, не открывая дверь, поднести карту с другой и, пока система запирает замок с одной стороны и отпирает с другой, одновременно синхронно (с точностью до нескольких миллисекунд) дернуть обе двери, то они откроются, и шлюз остается открытым, гуляй – не хочу. Я думал, это статистически невозможно. Однако изнывающие от безделья солдаты после месяца ежедневных тренировок мне на бис показывали, как легко обойти все хитроумные алгоритмы.

Изощренный шлюз

Встречаются в жизни и предельно изощренные варианты шлюза. Например, в упомянутых алмазных шахтах в ЮАР шлюз представляет собой изломанный коридор с несколькими дверями и турникетами. Пока первый человек не пройдет его до конца, второй не войдет в него. Таким образом они защищаются от "пробрасывания" алмазов навстречу движению, когда бригада идет на смену.

Впрочем, говорят, и это не очень помогает – просто каждый идущий перебрасывает мешочек через одну дверь пока в нее проходит, следующий – через другую, и так далее.

Конечно, тут необходимо организовать сговор именно нескольких человек подряд, однако такое вполне возможно – проходят бригадами, вся бригада обычно набрана из одной деревни, сватья-братья, им и сговариваться не надо.

Дополнительным бонусом от установки турникетов и шлюзов, замедляющих проход, будет защита от силового вторжения группы вооруженных людей. Даже если они заставят кого-то пропустить их, через ряд турникетов физически количеству людей – есть шанс, что поднятые (разбуженные) по тревоге дежурные сотрудники охраны успеют оказать сопротивление.

Недисциплинированные сотрудники, которым не нравится, что шлюзы замедляют проход, все равно могут все испортить.

Если вход осуществляется через турникет, то для проноса новой мебели должен быть отдельный проход с дверью (порой это не дверь, а настоящие ворота). Когда сотрудникам надоедает медленно ходить через шлюз, они берут у завхоза ключ от "грузовой двери", открывают эти ворота и ходят через них, вообще не затрудняя себя никакими правилами доступа.

Электроника против народных средств

Итак, резюмируя, могу сказать, что все электронные ухищрения сейчас являются просто реализацией на новой технологической базе старых правил доступа, проверенных веками. Однако и старые способы обходить правила, также изменившись, продолжают применяться. Так что без согласия и дисциплинированного сотрудничества персонала объекта все усилия по ужесточению алгоритмов доступа будут тщетны. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru