**Техника развивается, электроника дешевеет, однако в части контроля доступа за 20 лет произошло не так уж много нового. Да, достаточно широко стали применяться биометрические считыватели. Да, применяются смарт-карты или перезаписываемые карты. Но это фактически никак не сказывается на применяемых алгоритмах, оба упомянутых новшества являются чисто технологическими: повышают надежность и защищенность идентификаторов доступа**

Алексей Омельянчук
Начальник КБ компании "Сигма ИС"

# Особые алгоритмы доступа для особо важных объектов

Действительно, отпечаток пальца или рисунок глаза украсть и подделать труднее, чем обычную карту. Карту с шифрованным обменом, да еще и с плавающим перезаписываемым кодом также труднее незаметно прочитать в чужом кармане и потом подделать.

Алгоритмы же, применявшиеся для повышения защищенности особо важных объектов, практически не изменились и поныне. Хорошая новость – они теперь доступны даже в недорогих массовых системах. Плохая новость – их применение настолько осложняет повседневные процедуры, что такие алгоритмы реально уместно применять только на таких объектах, где весь персонал понимает и принимает необходимость жесточайших мер.

Какие же существуют алгоритмы повышения защиты?

Основных идей три: зональный Antipassback, комиссионность, участие оператора.

## Зональный Antipassback

Первая – зональный, рубежный или маршрутный контроль. Он же "Antipassback по областям". Названия и методики настройки в разных системах отличаются, но суть одна: чтобы пройти в нужную дверь, человек, имеющий на это право, должен перед этим пройти через одну или несколько предшествующих дверей. Нарушение правила означает, что, вероятно, кто-то прошел по другой карте во внешнюю дверь, а теперь по этой карте (вероятно, украденной) пытается пройти в особо секретную дверь. Заодно исключается возможность передачи карты – когда, скажем, кассир, сидя в столовой, дает свою карту подружке, мол сбегай, принеси забытую пудреницу. Частный случай, дополнительно усиленный совмещением разных технологий идентификации, – это шлюз, когда после входа в шлюзовую кабину надо в течение заданного времени предъявить другой идентификатор (обычно биометрический), после чего выйти из кабины далее на территорию. В доведенном до предела (или до абсурда?) алгоритме шлюза, применяемом на алмазных шахтах "Де Бирс", используется последовательность из нескольких дверей, расположенных в изломанном коридоре, через который человек должен пройти за заданное время, при этом вернуться назад нельзя, только вперед, и снаружи никто не видит, на какой стадии идущий. Там это обеспечивает также невозможность по предварительному сговору организовать переброс украденных алмазов навстречу движению через входной коридор, не оснащенный рентгеновской установкой контроля выноса алмазов. Говорят, все равно воруют, но это требует сговора очень большого количества людей, что легче расследовать.

## Комиссионность

Вторая идея – комиссионность. Для вскрытия хранилища обогащенного урана или входа в цех сортировки алмазов (где алмазы лежат еще не пересчи-

**Алгоритмы же, применявшиеся для повышения защищенности особо важных объектов, практически не изменились и поныне. Хорошая новость – они теперь доступны даже в недорогих массовых системах. Плохая новость – их применение настолько осложняет повседневные процедуры, что такие алгоритмы реально уместно применять только на таких объектах, где весь персонал понимает и принимает необходимость жесточайших мер.
Какие же существуют алгоритмы повышения защиты?
Основных идей три: зональный Antipassback, комиссионность, участие оператора**

танные, но уже внавал в больших ящиках) должны присутствовать как минимум двое, а то и трое доверенных лиц одновременно. И выйти из такого помещения можно только всем троим одновременно – ни в какой момент нельзя, чтобы в помещении осталось меньше заданного количества людей. В простом варианте требуется именно количество людей, имеющих право находиться в помещении, – скажем, всегда не меньше трех. В более сложных случаях требуется, чтобы хотя бы один из людей был, скажем, из службы главного технолога, еще хотя бы один – из службы безопасности, и еще один – из числа контролеров-учетчиков. Если же в какой-то момент в помещении осталось даже десять сотрудников безопасности и ни одного технолога – уже тревога, ибо вероятность сговора внутри одной службы значительно выше, чем между службами. Доведенные до абсурда варианты предусматривают, как при пуске ядерных ракет, одновременное предъявление карт или биометрических признаков на нескольких считывателях, разнесенных больше чем на два метра, – чтобы один сошедший с ума капитан подлодки в принципе не смог запустить ракету.

Вариант комиссионности – посещение объекта с сопровождающим. Посетителю выдают карточку, она дает право на проход в некоторые двери, но в режимных зонах она действует, только если одновременно с ней предъявляется карта сопровождающего. Сотрудника, назначенного сопровождающим, также система не пропустит, если он "забыл" своего подопечного в режимной зоне. В столовой – на здоровье, можно посетителю находиться без присмотра. А в реакторном зале – только в сопровождении специально назначенного сопровождающего.

## Участие оператора

Наконец, третий алгоритм – участие оператора. Простейший вариант – так называемая фотоидентификация. Человек прикладывает карточку к считывателю, вахтеру на экран компьютера выводится фотография из личного дела, на соседнем видеомониторе изображение с видеокамеры того человека, который приложил карточку, и если все ок, вахтер нажимает кнопку и турникет, наконец, открывается. Это похоже на совмещение считывателя карты с системой распознавания лиц. Но, во-первых, вахтер (человек) все-таки значительно лучше может распознавать лица, во-вторых, его нельзя обмануть фотографией лица (что проходит с большинством систем автоматического распознавания), а главное, существуют и доведенные до абсурда варианты участия оператора: в том же славящемся своими мерами безопасности "Де Бирс" для доступа к аппаратам обогащения – в них могут быть алмазы на виду, а любые аппараты надо иногда чистить, регулировать и т.д. – так вот, для доступа туда требуется не только предъявить карту на считывателе, но и набрать код, указывающий, какие работы предполагается провести. У оператора на экране выводится посекундный график действий человека, и оператор наблюдает через видеокамеру, чтобы работник делал именно то, что заявлено, а не ковырялся в налипшей на кожух массе, выискивая особо крупные брильянты.

## Подводные камни

Следует отметить общее у всех подобных алгоритмов – их неудобство. Зональный Antipassback требует обязательно всегда прикладывать карточку. Если идут два друга, беседуют, один приложил карточку, открыл дверь, а второй прошел с ним вместе и забыл приложить карту, или приложил, но она не считалась, а он не заметил – дверь-то все равно уже открыта – и прошел, то в результате, когда они разойдутся по делам, система не выпустит второго из области – ведь с ее точки зрения он туда не входил, а значит, и выходить ему не положено. Такие ситуации возникают сплошь и рядом при попытке включить зональный Antipassback. Типичная рекомендация – использовать такой контроль только на точках доступа, оснащенных турникетами – там труднее случайно пройти вдвоем. Комиссионность и подавно вызывает жуткие неудобства. Работают трое, одному понадобилось выйти по нужде, так остальным придется тоже прервать работу, выйти из режимного помещения и подождать пока он не вернется.

Я уж не говорю про участие оператора. Если оператор отвлекся, не дает своего разрешения, а на станке порвался ремень привода и его срочно надо заменить, спасают только расставленные повсюду интеркомы, через которые можно срочно наорать на оператора службы безопасности, а если надо – то и нажаловаться его начальнику.

В целом, как уже отмечалось, основные алгоритмы повышения защиты особо важных объектов неизменны. Даже не 20 лет, когда используются более-менее современные системы доступа, а лет 100 – когда еще не было никакой электроники, а все пропуска проверялись караульными. Все равно действовали те же алгоритмы – зональность (на предыдущем посту надо было взять карточку о проходе и предъявить на следующем), комиссионность (караульных стояло по два, из разных служб, и они проверяли, чтобы проходили внутрь только по трое). И конечно, участие оператора, когда при доступе в особое помещение на специальную галерею выходил автоматчик и наблюдал, чтобы работники не отвлекались от работы. Все это лишний раз подтверждает тот факт, что безопасность обеспечивают люди и взаимный контроль людей друг за другом. А техника лишь помогает более четко организовать такой взаимный контроль.

**All-over-IP'2014**

19–20 ноября, КВЦ "Сокольники"

Приглашаем производителей, поставщиков, системных интеграторов и заказчиков систем контроля и управления доступом обсудить профессиональные вопросы на форуме All-over-IP Expo 2014.

**Бронируйте сегодня на лучших условиях!**
www.all-over-ip.ru