УДК 004.056

О защите билетов на электронных носителях от подделки

А.В. Уривский

ОАО «ИнфоТеКС»

Билеты на электронных носителях активно заменяют билеты на бумажных носителях. При очевидных экономических и пользовательских достоинствах применение электронных носителей несет и новые угрозы безопасности.

Одной из серьезных угроз традиционным билетам было незаконное тиражирование. При автоматической проверке достаточно было создать ксерокопию билета. Причем дешевого способа борьбы с этой угрозой не известно. Для случая ручной проверки традиционно билеты печатались на защищенных бланках с некоторым набором физических защитных механизмов – специальные краски, специальные материалы, голограммы и т.п. Другой угрозой была фабрикация билетов, когда злоумышленник, выяснив правила формирования содержимого билета, создавал свой собственный билет. Защищенные бланки не помогают для борьбы с этой угрозой, но в автоматических системах борьба ведется с применением криптографических средств аутентификации – кодами аутентификации сообщений или электронной подписью билетной системы [1].

Для электронных билетов физическая защита носителя обычно не является целевой задачей. Это связано с использованием полностью автоматических систем продажи и проверки билетов, в которых проверка защитных признаков практически не производится. Однако даже в предположении, что данные, составляющие билет, защищены, возникает ряд угроз самому электронному носителю как хранилищу данных и несанкционированному доступу к нему. Во-первых, при незащищенном носителе, например обычной флэш-памяти, возможен перенос билета на другой носитель и его неограниченное тиражирование. Во-вторых, возможно многократное воспроизведение одних и тех же данных, выдаваемых за актуальные. Это так называемая replay-атака особенно актуальная в случае, когда носителе размещается относительно универсальный электронный кошелек. В этом случае replay-атака приводит к восстановлению предыдущего состояния кошелька, что можно интерпретировать как незаконное его пополнение.

Один из простейших методов борьбы с указанными угрозами заключается в том, что при каждом использовании билета проверяется соответствие его состояния ожидаемому. Такая защита требует создания либо базы использованных билетов («черных» списков), либо базы текущего состояния всех билетов в билетной системе и поддержания этих баз в актуальном состоянии. В масштабных билетных системах проблему может представлять как оперативность загрузки элементов этих баз в устройства проверки, что сводится к требованию постоянного наличия связи базы и устройств, так и размер элементов баз, что предъявляет требования к пропускной способности упомянутых каналов связи.

Другой подход состоит в разработке средств, блокирующих перенос билета с одного носителя на другой и защиту от несанкционированного изменения содержимого носителя. По сути, речь идет о механизмах защиты от отчуждения информации от носителя и от несанкционированного доступа. Наиболее эффективным методом защиты представляется использование криптографических механизмов защиты информации. В этом случае как носитель билета, так и считыватель должны являться криптографическими модулями, например смарт-картами, которые защищенным образом хранят свои криптографические параметры (ключи) и реализуют криптографические преобразования. Для защиты билетов могут применять как одноключевые (симметричные) криптомеханизмы, так и двухключевые (асимметричные). В первом случае носитель и считыватель должны владеть одинаковым ключом, с помощью которого данные могут зашифровываться и вычисляться коды аутентификации сообщений. Во втором случае у каждого из объектов имеется собственная ключевая пара – закрытый и открытый ключи, – которые можно использовать в схеме электронной подписи или в процедуре выработки общего закрытого ключа типа протокола Диффи-Хеллмана. Реализации на современных носителях, типичных для билетной тематики, симметричных механизмов обладают высоким быстродействием (скорости обработки в десятки кбайт/с) и относительно компактны (единицы килобайт). Асимметричные – медленнее (единицы операций в секунду) и занимают существенный объем (десятки килобайт) или требуют криптосопроцессора. Проблема использования симметричных механизмов в том, что объектов, имеющих доступ к одному и тому же ключу,

оказывается много. Например, все считыватели системы должны владеть, или уметь вычислять, ключ доступа к конкретному носителю. Это повышает вероятность компрометации ключа.

Для борьбы с тиражированием билет, как структура данных в электронном виде, должен быть «привязан» к своему носителю. Обычно это достигается введением уникальных параметров носителя, например идентификатора кристалла, в состав билета, который защищается, упомянутыми выше методами обеспечения аутентичности. При построении системы на защиты на основе симметричных криптомеханизмов ключи защиты/доступа могут модифицироваться номером кристалла.

Для защиты от клонирования носителя или подмены носителя, когда злоумышленник пытается воспроизвести уникальные признаки на другом носителе, необходимо при считывании проводить аутентификацию носителя считывателем. Это может быть реализовано с использованием электронной подписи, а также с помощью кодов аутентификации сообщений.

Наиболее эффективными на сегодняшний день являются replay-атаки. Для борьбы с ними предлагается использовать два подхода.

Во-первых, обеспечить актуальность (freshness) обмена между носителем и считывателем. Известны три способа такого обеспечения: использование меток времени, счетчиков и одноразовых случайных чисел (nonce). Метки времени из-за отсутствия системных часов на носителе, очевидно, не применимы. Использование счетчиков возможно в случае их аппаратной реализации на носителе, причем желательно однонаправленных. В этой работе предлагается использование именно nonce при установлении соединения между носителем и считывателем. Т.е. сторона, намеревающаяся установить аутентичной другой стороны, добавляет в состав уже защищенного протокола случайное число. Ответ аутентифицируемой стороны должен содержать в своем составе некоторую заранее известную функцию от полученного случайного числа. Принципиальным здесь является как случайность nonce, так и то, что его использование должно быть защищено электронной подписью или кодов аутентификации. Внедрение nonce в состав протоколов аутентификации превращает их в протоколы класса «запрос-ответ». Для практики важным является длительность полного цикла взаимодействия носитель-считыватель. В худшем случае при использовании nonce к уже реализованному протоколу защиты может добавиться полный раунд обмена (две посылки, по одной в каждую сторону). Наши оценки и эксперименты показывают, что для современных карт, даже при бесконтактном считывании, дополнительная задержка не превосходит десятков миллисекунд.

Во-вторых, гарантировать то, что только доверенный считыватель может размещать билет на носителе. То есть необходимо обеспечить аутентификацию считывателя носителем. В целом такая аутентификация может реализовываться аналогично аутентификации носителя считывателем. Как отмечено выше, более предпочтительным является использованием асимметричных криптомеханизмов, в частности электронной подписи. Однако что в отличие от считывателя, у носителя, как правило, нет собственного источника питания и системных часов, поэтому имеется риск прохождения считывателем аутентификации по отозванной электронной подписи. При таких предположениях, сертификаты считывателя должны иметь очень ограниченных срок действия, а носитель периодически должен взаимодействовать с гарантированно аутентичным считывателем для загрузки «свежих» сертификатов и уточнения оценки текущего времени. Кроме того, операция проверки подписи – вычислительно емкая процедура. К тому потребуется, как минимум, две таких проверки: для проверки сертификата считывателя и проверки ответа считывателя, включающего функцию от nonce. Наши оценки показывают, что на современных носителях, одна проверка подписи может занимать порядка 200 мс или меньше.

Таким образом, одновременное использование предлагаемых подходов может привести к увеличению полного цикла на 500 мс. Вопрос допустимости такой задержки в каждой конкретной системе должен рассматриваться отдельно. Отметим, что сейчас это находится на грани допустимого для билетных систем пригородных поездов и метрополитена. С развитием технологий, безусловно, острота ограничений будет падать.

Наиболее концептуально близкой и доведенной до широкого применения реализацией защиты является технология машиносчитываемых проездных документов (machine readable travel document) [2], разработанная ИКАО для защиты электронных паспортов и виз.

Литература

1. Уривский А. В. О криптографической защите билетов // T-Comm –Телекоммуникации и Транспорт. – 2012. – Специальный выпуск – «Комплексная безопасность». – С. 31–33.
2. *ICAO Doc 9303* Machine Readable Travel Documents, Part 1: Machine Readable Passport. – 2006.