УДК 004.056

Система криптографических ключей для защиты билетов от подделки

А.В. Уривский

ОАО «ИнфоТеКС»

Защита билетов на бумажных носителях от тиражирования с использованием криптографических средств является весьма актуальной и технически содержательной [1].

В данной работе мы рассматриваем задачу построения системы управления криптографическими ключами при использовании криптографических кодов аутентификации сообщений (имитовставок). Суть защиты состоит в том, что для сообщения (билета) M и секретного ключа k вычисляется имитовставка $A=MAC(M,k)$, которая передается и хранится вместе с сообщением. Проверка подлинности состоит в том, что по полученным, возможно искаженным, сообщению M^* и коду A^* получатель, используя известный ему ключ, вычисляет оценку $MAC^*(M^*,k)$. Если $A=MAC^*(M^*,k^*)$, то получатель полагает, что сообщение подлинное, иначе – поддельное.

Основной практической угрозой данного класса методов является то, что устройства формирования и проверки билетов используют одни и те же секретные ключи. Поэтому задача управления ключами в рассматриваемом случае состоит в том, чтобы снизить вероятность компрометации секретного ключа.

Простая мера состоит в прямом ограничении числа устройств, имеющих доступ к конкретному ключу. Это достигается объединением устройств в группы по некоторому признаку F, например по обслуживанию конкретного мероприятия, маршрута транспорта и т.п., и назначению отдельного ключа каждому допустимому значению признака R.

Более эффективной мерой является диверсификация (вычисление производных) ключей. Суть ее в том, чтобы на устройствах формирования билетов (кассах) использовать ключи, производные от тех, которые используются на устройствах проверки (турникетах). Основа для именно такой диверсификации в том, что, во-первых, как правило, устройств формирования существенно больше, чем устройств проверки, а, во-вторых, устройства проверки чаще всего размещаются в некоторой контролируемой зоне, доступ в которую злоумышленника сильно ограничен. Поэтому именно устройства формирования в большей степени влияют на компрометацию.

Производный ключ k_C получается из исходного ключа k путем применения так называемой псевдослучайной функции: $k_C = f(k,C)$ [2]. Здесь данные C однозначно определяют конкретное устройство формирования, например являются идентификатором. В результате в силу свойств псевдослучайной функции для злоумышленника производный

ключ выглядит случайным по отношению к исходному. Как следствие, злоумышленник не может вычислить ни исходный ключ, не вычислить производный ключ другого устройства. Таким образом, ключ k_C можно считать персонализованным для устройства *C*. Устройство формирование владеет только персонализованным ключом k_C, а устройство проверки исходным ключом *k*. При этом на момент проверки имитовставки устройство проверки вычисляет из ключа *k* ключ k_C по известному значению *C*.

В ряде случаев диверсификации ключей не достаточно для обеспечения низкой вероятности компрометации. В частности, на практике встречаются случаи, когда устройства формирования и проверки физически совмещены, например в мобильных терминалах кассира. Упомянутая мобильность не позволяет сделать предположение о наличии защищенного периметра, в котором находится устройство проверки. В этом случае предлагается проводить процедуру многостадийной диверсификации ключей. В стационарных устройств проверки используется исходный ключ *k*, а в мобильных – ключ $k_B = f(k,B)$, где B – некоторый идентификатор, относящийся ко всем мобильным устройствам. Каждому устройству формирования, как стационарному, так и мобильному, выдается по два ключа k_C и $k_{BC} = f(k_B,C) = f(f(k,B),C)$.

При формировании билета устройство формирования вычисляет две имитовставки для одного и того же сообщения: одну на ключе k_C, другую на ключе k_{BC}. При проверке мобильное устройство проверки проверяет только имитовставку, вычисленную на ключе k_{BC}, а стационарное устройство проверяет обе имитовставки.

Для криптографически стойкого алгоритма $MAC(M,k)$, например реализованного использованием блочного шифра в соответствующем режиме работы или ключевой хэш-функции, и длине имитовставки в *l* бит, вероятность формирования злоумышленником имитовставки, которая может пройти проверку, без знания ключа составляет 2^{-l}. Поэтому вероятность навязывания поддельного билета мобильному устройству проверки оказывается выше, чем стационарному. Однако это может быть компенсировано тем, что оператор мобильного устройства может дополнительно учитывать защитные признаки физического носителя билета – водяные знаки, специальные краски и т.п.

Литература

1. *Уривский А. В.* О криптографической защите билетов // T-Comm –Телекоммуникации и Транспорт. – 2012. – Специальный выпуск – «Комплексная безопасность». – С. 31–33.
2. *Goldreich O., Goldwasser S., Micali S.* On the Cryptographic Applications of Random Functions (Extended Abstract) // Advances in Cryptology – Proceedings of CRYPTO’84. – 1985. – LNCS 196. – P. 276–288.