В. А. Конявский, д. т. н.,

зав. кафедрой «Защита информации» ФРТК МФТИ,

А. М. Коротин, аспирант НИЯУ МИФИ

Доверенная информационная среда и противодействие подмене данных и атакам на каналы управления

Как можно противодействовать подмене данных и как бороться с атаками на каналы управления – вовсе не секрет: все можно зашифровать и все подписать. Только не всегда это можно сделать. Как правило, пропускная способность каналов управления очень ограничена, и объем данных сигналов управления в общем случае значительно меньше, чем у электронной подписи (ЭП). Защищенность обеспечивается избыточностью, но в ряде случаев избыточность не может быть большой.

В этой статье мы рассмотрим, что можно предпринять при этих ограничениях.

Для анализа возможных способов противодействия атакам по подмене данных воспользуемся понятием доверенной среды и связанными с ним определениями. В соответствии с [1]:

1. **Защищённая информационная технология** – информационная технология, обладающая свойством сохранять последовательность операций.
2. **Среда функционирования ИТ** – совокупность технических средств исполнения информационных операций, включая каналы связи.
3. **Доверенная среда функционирования** – взаимодействующая совокупность доверенных узлов обработки данных.
4. **Доверенный узел обработки** – выделенная совокупность аутентифицированных и целостных технических средств с проверенным программным обеспечением.

Принцип, что в доверенной среде все должно быть доверенным, показан в работе [1-1]. Для корпоративных или локальных систем обеспечение доверенности входящих в их состав узлов является, как правило, достаточным для того, чтобы считать всю систему доверенной. С появлением открытых систем стал актуальным вопрос обеспечения доверенности каналов связи (транспортной среды), которые в большинстве своем принадлежат другим собственникам с другими целями и совсем не обязательно являются доверенными.

Для того чтобы канал связи стал доверенным, необходимо, как минимум, знать «куда» и «откуда» передается информация. Следовательно, узлы при взаимодействии по каналу связи должны быть аутентифицированы. Кроме того, возможны ситуации, в которых необходимо обеспечивать конфиденциальность и целостность передаваемой информации. Таким образом, согласно [1]:

Каналы связи в доверенной среде функционирования *должны* быть аутентифицированы и *могут* быть защищены.

Для аутентификации узлов в канале связи с обоих сторон должны применяться активные элементы. Если передаваемая по каналам связи информация является конфиденциальной, то для ее защиты может применяться шифрование. В этом случае возникает задача управления ключами, решение которой для системы с большим количеством распределенных узлов является достаточно сложным. В результате сложность будет снята с задачи защиты канала связи, но перенесена на задачу построения системы управления ключами.

Существуют каналы связи, не нуждающиеся в обеспечении конфиденциальности передаваемых в них данных. В частности, к таким каналам относят каналы управления, характеризующиеся, как отмечалось в начале статьи, малой пропускной способностью. Для защиты таких каналов

могут использоваться защитные коды аутентификации (ЗКА) – блоки данных, добавляющиеся к концу сообщений для контроля их целостности и аутентификации источника их отправки. Для формирования ЗКА могут использоваться симметричные алгоритмы шифрования или функции хэширования. В первом случае вырабатывается имитовставка, во втором – HMAC. Защитный код аутентификации формируется путем отбора достаточного количества байт из имитовставки или HMAC. По сравнению с электронной подписью применение ЗКА приводит к меньшей избыточности в канале управления, что является крайне важным при ограничении имеющихся технико-экономических ресурсов.

Для понимания принципа достаточности длины ЗКА рассмотрим классическую задачу о днях рождения. Требуется определить вероятность, при которой в группе из k человек как минимум у двоих совпадут дни рождения. Одно из возможных решений данной задачи связано с нахождением величины $\bar{p}(k)$ – вероятности, что у всех членов группы дни рождения будут различными. Так как вероятность несовпадения дней рождения для двух случайно выбранных людей равна $p_2 = 1 - \frac{1}{365}$, для трех $p_3 = (1 - \frac{1}{365})(1 - \frac{2}{365})$ и так далее, то вероятность несовпадения для всех членов группы равна:

$$\bar{p}(k) = = \left(1 - \frac{1}{365}\right)\left(1 - \frac{2}{365}\right) \dots \left(1 - \frac{k-1}{365}\right) = \frac{365!}{365^k(365-k)!}$$

Учитывая, что искомая вероятность совпадения дней рождения у любых двоих членов группы равна $p(k) = 1 - \bar{p}(k)$, нетрудно найти решение задачи для различных k.

В контексте применения ЗКА для канала управления, задача о днях рождения может быть сформулирована следующим образом: требуется определить вероятность коллизии значений ЗКА для любых двух сообщений в течение времени действия ключа генерации ЗКА. При такой формулировке количество различных сообщений будет эквивалентно числу людей в группе,

а количество дней в году – величине N, общему числу возможных ЗКА заданной длины.

Для решения поставленной задачи можно найти вероятность неповторения ЗКА в течение времени действия ключа. Аналогичный подход используется и в классической задаче о днях рождения. Тогда, используя разложение экспоненциальной функции в ряд Тейлора: $e^x = 1 + \sum_{n=1}^{\infty} \frac{x^n}{n!}$ и учитывая большой размер чисел N и k, вероятность неповторения ЗКА для k сообщений будет равна:

$p(n) = 1 - \frac{k^2}{2N}$, $N = 2^{8m}$, где m – длина ЗКА в байтах.

Приведем пример использования полученной формулы. Пусть по каналу связи раз в 30 секунд передается команда управления. Тогда в течение периода действия ключа генерации ЗКА (например, 1 год) по каналу связи будет передано $k = 2 * 60 * 24 * 365 \approx 10^6$ сообщений. Перебирая разные значения m, можно определить вероятность коллизии для любых двух сообщений в течение одного года при заданной длине ЗКА. Так для $m = 6$ вероятность коллизии будет равна: $1 - p(n) = 3 * 10^{-9}$, что согласно экспертной оценке [2] является допустимым значением. Следовательно, длина ЗКА, равная 6 байтам, является достаточной для обеспечения защиты приведенного в примере канала связи. По сравнению с использованием ЭП в соответствии с ГОСТ 34.10-2012 избыточность была уменьшена более, чем в 10 раз.

Низкая вероятность коллизий ЗКА для двух любых сообщений позволяет минимизировать вероятность атаки, при которой злоумышленник перехватывает два сообщения с одинаковым ЗКА и меняет их смысловые части местами.

Защитные коды аутентификации нашли своей применение в системе контроля целостности и подтверждения достоверности (СКЦПД) электронных платежей в банковской сфере. Что касается каналов управления, то на

сегодняшний день ведутся работы по созданию аналогичной СКЦПД в сфере железнодорожного транспорта для системы автоматической локомотивной сигнализации [3], использующейся для передачи на бортовые локомотивные устройства информации о допустимой скорости движения и дополнительных условиях следования железнодорожного подвижного состава: разрешение на движение, ограничение скорости, маршрут движения по железнодорожной станции [4]. При этом в качестве канала связи предполагается использование радиоканала DMR-RUS, обладающего низкой пропускной способностью.

Список литературы:

[1] Доверенные системы как средство противодействия киберугрозам. Базовые понятия.

[2] Конявский В.А. Управление защитой информации на базе СЗИ НСД «Аккорд». – М.: Радио и связь, 1999. – 325 с.

[3] Valery Konyavskiy, Anna Epishkina, Alexander Korotin. The design of integrity monitoring and reliability verification system for critical information, transmitted in automatic train signaling system, based on DMR-RUS radio channel. Procedia Computer Science, Volume 88C, 2016, Pages 318-323.

[4] ГОСТ Р 53431-2009. Автоматика и телемеханика железнодорожная. Термины и определения (с Изменением № 1). – Введ. 2011-01-01. – М.: Стандартинформ, 2010. – 24 с.