§ 2.2. Управление секретными ключами

Порядок использования криптографической системы определяется системами установки и управления ключами.

Система установки ключей определяет алгоритмы и процедуры генерации, распределения, передачи и проверки ключей.

Система управления ключами определяет порядок использования, смены, хранения и архивирования, резервного копирования и восстановления, замены или изъятия из обращения скомпрометированных, а также уничтожения старых ключей.

Предварительное распределение ключей

Для надежной защиты информации, передаваемой по открытому каналу связи, применяют криптографические средства. Чтобы воспользоваться ими, необходимо осуществить первоначальный выбор и установку ключей. Для генерации ключей могут применяться различные алгоритмы. Выбранные ключи необходимо как-либо передать взаимодействующим сторонам. Поэтому для первоначального распределения ключей необходим защищенный канал связи.

Самый надежный способ первоначального распределения ключей — это личная встреча всех взаимодействующих сторон. Можно использовать также специальных курьеров, которые будут развозить ключи. Однако при большом числе

взаимодействующих сторон требуется предварительная рассылка значительного объема ключевой информации и последующее ее хранение. Поэтому на практике применяют специальные *системы предварительного распределения ключей*, предусматривающие распределение и хранение не самих ключей, а некоторой меньшей по объему исходной информации, на основе которой в дальнейшем каждая сторона может вычислить ключ для взаимодействия с другой стороной. Система предварительного распределения ключей включает два алгоритма. С помощью первого алгоритма осуществляется генерация исходной информации. Эта информация включает открытую часть, которая будет передана всем сторонам или помещена на общедоступном сервере, а также секретные части каждой стороны. Второй алгоритм предназначен для вычисления действующего значения ключа для взаимодействия между абонентами по имеющейся у них секретной и общей открытой части исходной ключевой информации.

Система предварительного распределения ключей должна быть *устойчивой*, то есть учитывать возможность раскрытия части ключей при компрометации, обмане или сговоре абонентов, и *гибкой* — допускать возможность быстрого восстановления путем исключения скомпрометированных и подключения новых абонентов.

Пересылка ключей

После того как предварительное распределение ключей произведено, может потребоваться передача ключей для каждого конкретного сеанса взаимодействия. Передача этих ключей может осуществляться с помощью шифрования с использованием ранее полученных ключей.

Для передачи зашифрованных ключей по открытому каналу связи между не доверяющими друг другу абонентами требуется решение всего комплекса задач по установлению подлинности различных аспектов взаимодействия, начиная от подлинности субъектов взаимодействия, подлинности пере-

даваемых сообщений, подлинности самого сеанса связи и кончая подтверждением правильности (идентичности) полученных абонентами ключей.

Для централизованного управления пересылкой ключей создаются специальные доверенные центры, выполняющие функции центров распределения или перешифрования ключей. Различие между этими центрами заключается в том, что в первом случае генерация ключей осуществляется в центре распределения, а во втором случае — самими абонентами.

Открытое распределение ключей

Наиболее просто распределение ключей осуществляется в *системах открытого распределения (секретных) ключей.* Для сетей связи с большим числом абонентов традиционные подходы к построению системы распределения ключей оказываются очень неудобными. Диффи и Хеллман впервые показали, как можно решить эту задачу, используя незащищенный канал связи.

В предложенной ими системе открытого распределения ключей [Диф79] каждая из сторон изначально имеет свой секретный параметр. Стороны реализуют определенный протокол взаимодействия по открытому каналу связи. При этом они обмениваются некоторыми сообщениями (образованными с помощью своих секретных параметров) и по результатам этого обмена вычисляют общий секретный связной ключ. В более поздних работах такие протоколы стали называть *протоколами выработки общего ключа*, поскольку изначально ни одна из сторон не имеет ключа и как такового распределения или пересылки ключей в нем не происходит.

В исходном виде система Диффи и Хеллмана имела существенные недостатки, связанные с возможностью для третьей стороны по осуществлению активного вхождения в канал связи и проведению полного контроля передаваемой информации. Однако после небольших модификаций и дополнений их протокол уже позволяет осуществлять не только

выработку общего ключа, но и одновременно проверять и подтверждать правильность вычислений, а также проводить взаимную аутентификацию взаимодействующих сторон.

Схема разделения секрета

Еще одной задачей современной криптографии, тесно связанной с проблемой распределения ключей и активно развивающейся в последние годы, является задача построения *схем разделения секрета.* Для многих практически важных приложений, связанных с запуском или активизацией критических процессов или определяющих порядок получения доступа к значимым данным, ответственное лицо должно ввести секретный ключ. Чтобы обезопасить процедуру принятия решения и не отдавать все на волю одного человека, являющегося обладателем ключа, используют метод разделения секрета. Он состоит в назначении определенной группы лиц, которая имеет право принимать решение. Каждый член группы владеет определенной долей секрета (точнее, специально выбранным набором данных), полная совокупность которых позволяет восстановить секретный ключ. При этом схема разделения секрета выбирается с таким условием, что для восстановления секретного ключа требуется обязательное присутствие всех членов группы, так как в случае отсутствия хотя бы одного из участников объединение долей оставшихся членов группы гарантированно не позволяет получить никакой информации о секретном ключе. Таким образом, *схема разделения секрета* определяется двумя алгоритмами, удовлетворяющими сформулированному выше условию: первый алгоритм определяет порядок вычисления значений долей по заданному значению секретного ключа, а второй предназначен для восстановления значения секрета по известным долям.

Задачу построения схемы разделения секрета можно обобщить

— либо путем введения так называемой *структуры доступа*, когда решение может приниматься не одной, а несколькими различными группами, причем часть из участников может наделяться правом "вето",

— либо путем добавления механизмов, позволяющих обнаружить обман или сговор участников,

— либо введением специального протокола распределения долей между участниками с подтверждением правильности полученной информации и аутентификацией сторон.

§ 2.3. Инфраструктура открытых ключей

Сертификаты

Создание цифровой подписи позволило решить проблему *сертификации открытых ключей*. Она заключается в том, что перед тем как использовать открытый ключ некоторого абонента для отправки ему конфиденциального сообщения, отправитель должен быть уверен, что открытый ключ действительно принадлежит этому абоненту. Открытые ключи необходимо очень тщательно обезопасить, в том смысле, что если сервер, на котором они хранятся, не обеспечивает их целостность и аутентичность, то злоумышленник имеет возможность, подменив открытый ключ одного из абонентов, выступать от его имени. Поэтому для защиты открытых ключей создаются специальные *центры сертификации*, которые играют роль доверенной третьей стороны и заверяют открытые ключи каждого из абонентов своими цифровыми подписями.

Сертификат представляет собой набор данных, заверенный цифровой подписью центра и включающий открытый ключ и список дополнительных атрибутов, принадлежащих абоненту. К таким атрибутам относятся: имена пользователя и центра сертификации, номер сертификата, время действия сертификата, предназначение открытого ключа (цифровая подпись, шифрование) и т. д.

Международный стандарт ISO X.509 определяет общую структуру сертификатов открытых ключей и протоколы их использования для аутентификации в распределенных системах.

Центры сертификации

Центр сертификации предназначен для регистрации абонентов, изготовления сертификатов открытых ключей, хранения изготовленных сертификатов, поддержания в актуальном состоянии справочника действующих сертификатов и выпуска списка досрочно отозванных сертификатов.

Для сетей с большим числом абонентов создается несколько центров сертификации. Центры сертификации объединяются в древовидную структуру, в корне которой находится главный центр сертификации, который выдает сертификаты подчиненным ему отраслевым центрам, тем самым обеспечивая доверие к открытым ключам этих центров. Каждый центр вышестоящего уровня аналогичным образом делегирует право выпуска сертификатов подчиненным ему центрам. В результате доверие сертификату открытого ключа каждого центра основано на заверении его сертификата ключом вышестоящего центра. Сертификаты главного центра подписывает сам главный центр.

Зная иерархию и подчиненность друг другу центров сертификации, можно всегда точно установить, является ли абонент владельцем данного открытого ключа.

Основная трудность при создании центров сертификации заключается в их юридическом статусе и потенциальных финансовых возможностях по выплате компенсаций за ущерб, понесенный в результате невыполнения подписанных цифровыми подписями с использованием сертификатов, выданных этим центром, договоров и контрактов, сорванных по причине отказов от цифровых подписей или их подделки.