ТЕМА 9. Алгоритмы обмена ключей и протоколы аутентификации

9.1. Алгоритмы распределения ключей с использованием третьей доверенной стороны

Понятие мастер-ключа

При симметричном шифровании два участника, которые хотят обмениваться конфиденциальной информацией, должны иметь один и тот же ключ. Частота изменения ключа должна быть достаточно большой, чтобы у противника не хватило времени для полного перебора ключа. Следовательно, сила любой криптосистемы во многом зависит от технологии распределения ключа. Этот термин означает передачу ключа двум участникам, которые хотят обмениваться данными, таким способом, чтобы никто другой не мог ни подсмотреть, ни изменить этот ключ. Для двух участников *A* и *B* распределение ключа может быть выполнено одним из следующих способов.

1. Ключ может быть создан *A* и физически передан *B*.
2. *Третья сторона* может создать ключ и физически передать его *A* и *B*.
3. *A* и *B* имеют предварительно созданный и недолго используемый ключ, один участник может передать новый ключ другому, применив для шифрования старый ключ.
4. Если A и B каждый имеют безопасное соединение с третьим участником *C, C* может передать ключ по этому безопасному каналу *A* и *B*.

Количество требуемых ключей зависит от числа участников, которые должны взаимодействовать. Если выполняется шифрование на сетевом или IP-уровне, то ключ необходим для каждой пары хостов в сети. Таким образом, если есть N хостов, то необходимое число ключей [N (N - 1)]/2. Если шифрование выполняется на прикладном уровне, то ключ нужен для каждой пары прикладных процессов, которых гораздо больше, чем хостов.

Третий способ распределения ключей может применяться на любом уровне стека протоколов, но если атакующий получает возможность доступа к одному ключу, то вся последовательность ключей будет раскрыта. Более того, все равно должно быть проведено первоначальное распространение большого количества ключей.

Поэтому в больших автоматизированных системах широко применяются различные варианты четвертого способа. В этой схеме предполагается существование так называемого центра распределения ключей (Key Destribution Centre - *KDC*), который отвечает за распределение ключей для хостов, процессов и приложений. Каждый участник должен разделять уникальный ключ с *KDC*.

Использование центра распределения ключей основано на использовании иерархии ключей. Как минимум используется два типа ключей: *мастер-ключи* и *ключи сессии*.