ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ РЕЖИМОВ БЛОЧНЫХ ШИФРОВ ДЛЯ "ПРОЗРАЧНОГО" ШИФРОВАНИЯ ФАЙЛОВЫХ СИСТЕМ

А.В. Недилько

"Прозрачное" шифрование файловой системы является одним из наиболее распространенных и надежных средств защиты информации в настоящее время. Суть метода состоит в том, что создается единый зашифрованный файл на физическом носителе информации (так называемый контейнер), в пределах которого (как обычного дискового раздела) стандартными средствами ОС создается и используется файловая система. Таким образом, для пользователя работа с зашифрованными данными не отличается от работы с обычными данными.

Большинство современных файловых систем делят хранимую информацию на секторы, и выполняют все операции посекторно. Это означает, что драйвер виртуального устройства, который осуществляет шифрование / дешифрование, должен шифровать каждый сектор независимо от других. Сектор обычно больше блока шифра, поэтому сектор шифруется как последовательность блоков; при этом применяется определенный режим шифрования.

Необходимость шифровать каждый сектор независимо, а также особенности организации файловых систем создают следующие специфические условия, значительно расширяющие возможности для успешной атаки:

– файловая система всегда содержит служебные данные, формат, расположение, и часто сами значения которых могут быть предугаданы;

– теоретически возможно попадание в руки "взломщиков" нескольких копий одного и того же сектора, зашифрованного одним ключом, но с различным инициализационным вектором;

– создавать случайные инициализационные векторы для каждого сектора нецелесообразно; вместо этого они вычисляются, а значит, могут быть вычислены и при взломе.

В этих условиях стандартные режимы шифрования (ECB, CBC, CFB, OFB, CTR) не обеспечивают достаточный уровень надежности.

Для обеспечения надежности защиты данных при шифровании файловых систем были разработаны специальные режимы шифрования: ESSIV, LRW, XEX, XTS. На сегодняшний день наиболее безопасным является режим XTS, который был сертифицирован IEEE в декабре 2007. Режим XTS уже используется в специализированном ПО для "прозрачного" шифрования файловой системы.