Отзыв на курсовую работу «Внедрение шифрование в систему хранения данных высокой производительности» студента 345 группы Овчинникова А. А.

Системы Хранения Данных оказывают все большее влияние во многие сферы жизни. В рамках предприятия СХД являются централизованными хранилищами, позволяющими гибко управлять информацией, обеспечивать надежность хранения, а также эффективно восстанавливаться после сбоев. Также усиливается тенденция хранения данных «в облаке», то есть в огромных дата-центрах, где вопрос сохранности информации критичен. Поэтому необходимо обеспечить СХД средством, позволяющим сберечь важные данные от посягательства третьих лиц. Одно из таких средств: шифрование данных. Внедрение данного механизма является нетривиальной задачей, особенно если стоит задача защитить уже эксплуатируемую СХД. Целью работы был ответ на вопрос: «Возможно ли эффективное внедрение в СХД механизма шифрования, отвечающего всем современным требованиям информационной безопасности?»

Сначала, разумеется, необходимо описать эти самые требования. Далее – исследовать специфику шифрования накопителей (в первую очередь, по сравнению с шифрованием, применяемым для передачи данных). Овчинниковым А.А. была проделана серьезная работа по исследованию как основных понятий и концепций современного шифрования (алгоритмы, режимы), так и существующих программных решений для защиты накопителей. Была предложена базовая концепция управления ключами, и рассмотрены механизмы встраивания в реальную систему. Из-за обширности предметной области в отчет вошли далеко не всё, что было изучено: был также описан ряд атак и проблем, возникающих при реализации шифрования в «лоб». Кроме того были рассмотрены решения сторонних производителей.

Осложнялась работа тем, что подавляющее большинство аналогичных решений рассчитано на крупных коммерческих потребителей, что приводит к недостатку - документации и спецификаций.

Что касается отчета, выполнен он довольно-таки опрятно, соответствуя практически всем требованиям, принятым для такого формата, выдержана структура.

К сожалению, из-за ограниченности времени, в реальную систему встроить шифрование не удалось. Но были выполнены тесты на искусственном стенде, где студент показал хорошее знание языка C и Intel intrinsics. Также студент показал умение разбираться в чужом коде, на примере ядра Linux (одним из этапов работы было исследование криптофункций ядра Linux).

Проведенная работа является только первым шагом. Следующим шагом будет применение полученных знаний и навыков при внедрении и тестировании в реальной СХД Avrora.

Ершов П.А.