УДК 004.056

ПРИМЕНЕНИЕ ХЕШИРОВАНИЯ В КРИПТОГРАФИЧЕСКИХ И НЕКРИПТОГРАФИЧЕСКИХ СИСТЕМАХ

Костенкова А.В.
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Научный руководитель – к.т.н., доцент Ли И.В.
Государственный университет морского и речного флота имени адмирала С.О. Макарова

В докладе представлен анализ распространенных методов применения хеширования, используемых для проверки целостности файлов и сообщений, и хранения парольных фраз в базах данных. Обоснована неактуальность применения старых методов и алгоритмов, а также приведены наиболее современные и надежные решения.

Введение. Хеширование, благодаря своим особенностям, позволяет реализовывать механизмы проверки целостности, ЭЦП, хранение паролей в базах данных, хеш-таблицы. Тем не менее, стоит понимать, что простота использования и реализации не всегда в приоритете, для достижения безопасности требуются новые и актуальные решения. Использование «чистых» хешей не рекомендуется, существуют новые механизмы, построенные на алгоритмах хеширования, но обеспечивающих лучшую безопасность.

Основная часть. Для анализа были выбраны 2 структуры, демонстрирующие использование криптографической и некриптографической хеш-функции. В первом случае выл сделан упор на криптостойкость механизма, во втором – на скорость и действенность реализации. Для рассмотрения некриптографических систем была выбрана одна из наиболее распространенных сфер применения хеш-функция – механизм проверки целостности сообщений или файлов. Стоит отметить, что тут будут выбраны различные решения, так как в одном случае было рассмотрен сценарий передачи информации между двумя лицами, а во втором – передача файлов в глобальной сети. В обоих случаях уже неактуально использовать только дайджест сообщения или файла. Все современные алгоритмы хеширования изначально проектируется быстрыми и легко реализуемыми, как на программном, так и на аппаратном уровнях, что удобно как для конечного пользователя, так и для злоумышленника, способного реализовать атаку перебора. Оптимальным решением будет использовать соль для хешей и функции формирования ключа, что, при грамотном использовании, позволит свести возможность получения злоумышленником парольных фраз к минимуму, сделав невозможными или практически невозможными все классические атаки при современных вычислительных мощностях.

Выводы. В результате исследования были проанализированы различные решения применения хеш-функций в механизмах проверки целостности файла или сообщения, и в реализации хранения парольных фраз в базах данных. Использование обычного дайджеста сообщения не гарантирует целостность сообщения, оптимальным решением будет использование механизма HMAC (hash-based message authentication code), проверка целостности и подлинности файлов на различных сайтах лучше реализовывается с использованием ЭЦП. Для хранения паролей так же сейчас недостаточно использовать даже самые последние алгоритмы хеширования, для обеспечения наибольшей сопротивляемости злоумышленникам требуется совмещать использование соли и функций формирования ключа.