Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н.Г.ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Система контроля целостности данных

АВТОРЕФЕРАТ

дипломной работы

студентки 6 курса 631 группы
специальности 090102.65 «Компьютерная безопасность»
факультета компьютерных наук и информационных технологий
Зубарь Дарьи Дмитриевны

Научный руководитель
доцент, к.ф.-м.н. А.В. Жаркова

Заведующий кафедрой
профессор, к.ф.-м.н. В.Н. Салий

Саратов 2016

ВВЕДЕНИЕ

В настоящее время существует такое понятие, используемое в контексте терминологии информационной безопасности, как «целостность объекта», причем объектом может быть информация, специализированные данные, ресурсы автоматизированной системы. Свойство целостности информации является одним из основных критериев информационной безопасности объекта.

Примерами нарушения целостности данных могут быть такие действия, как подделка документа, случайное изменение информации при передаче, изменение информации при неисправной работе жесткого диска, искажение фактов средствами массовой информации с целью манипуляции общественным мнением. В информационной безопасности и криптографии целостность данных в общем – это данные в том виде, в каком они были созданы. Для обеспечения целостности данных применяют различные методы, например, алгоритмы вычисления контрольной суммы, цифровой подписи и другие.

Целью данной выпускной квалификационной работы является рассмотрение существующих решений для контроля целостности данных, изучение функций хэширования, в частности ГОСТ Р 34.11-2012, и алгоритмов шифрования, в частности ГОСТ 28147-89, в результате чего требуется разработать и реализовать приложение для контроля целостности данных.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В первом разделе дипломной работы «Необходимые определения и сведения» определены основные понятия и приведены основные сведения, используемые в работе. Представлены определения таких терминов, как хэш-функция, блочный шифр, целостность данных и другие, а также были рассмотрены требования к криптографической хэш-функции и перечислены основные методы контроля целостности данных:

- полная копия данных;
- контрольная сумма;
- имитовставка;
- хэширование;
- электронная цифровая подпись.

В результате автором было выбрано хэширование в качестве метода контроля целостности данных.

Второй раздел «Функции хэширования» содержит общее описание хэш-функций, и в качестве примеров в нём рассмотрены функция хэширования SHA и отечественный стандарт функции хэширования ГОСТ Р 34.11-2012. В результате автором для реализации была выбрана функция хэширования ГОСТ Р 34.11-2012 с длиной хэш-кода 512 бит.

В третьем разделе работы «Блочные шифры» приведено общее описание блочных шифров и их достоинств, после чего подробно рассмотрены алгоритм шифрования AES и отечественный стандарт шифрования ГОСТ 28147-89, который и был выбран автором для реализации.

Следующий раздел называется «Обзор некоторых средств контроля целостности файлов». В нем рассмотрены некоторые доступные приложения, осуществляющие контроль целостности файлов (в частности, приложения EF CheckSum Manager и MD5 Checksum Tool), перечислены их особенности.

В пятом разделе «Разработанная система контроля целостности данных» описывается система контроля целостности данных «Stribog File Analyser», разработанная и реализованная автором в рамках данной дипломной работы (листинг программы приведен в приложении А). Описание включает в себя информацию о параметрах системы, на которой производилась сборка, и два режима работы разработанного приложения: режим пользователя и режим администратора. В данном разделе содержится подробное описание по использованию программы, сопровождающееся соответствующими снимками экрана. Также в конце раздела приведено сравнение разработанной системы со средствами контроля целостности файлов, которые были рассмотрены в предыдущем разделе, в частности, выявлены некоторые преимущества разработанного приложения.

ЗАКЛЮЧЕНИЕ

В рамках данной выпускной квалификационной работы были рассмотрены принципы работы систем контроля целостности данных, некоторые существующие доступные программы контроля целостности данных, изучены функции хэширования, в том числе отечественный стандарт ГОСТ Р 34.11-2012, алгоритмы шифрования, в том числе отечественный стандарт ГОСТ 28147-89. В результате проделанной работы была разработана и реализована система контроля целостности данных «Stribog File Analyser» на основании отечественных стандартов функции хэширования ГОСТ Р 34.11-2012 и алгоритма шифрования ГОСТ 28147-89.

Разработанная система может быть использована в двух режимах: в режиме администратора и в режиме пользователя. В режиме администратора реализованы следующие возможности: просмотр списка существующих пользователей, создание новых пользователей, генерация пользовательских ключей шифрования/расшифрования, изменение паролей пользователей и удаление пользователей. В пользовательском режиме система осуществляет контроль целостности данных следующим образом: при запуске программы в режиме пользователя происходит расшифрование всех его файлов, для составления базы хэш-кодов производится обход всех файлов в директории, принадлежащей пользователю, подсчитываются хэш-коды каждого файла и заносятся в базу хэш-кодов. При проверке целостности файлов проводится сравнение хэш-кодов файлов с хэш-кодами из базы. Несовпадение хэш-кодов говорит о том, что файл был каким-либо образом модифицирован; при этом система сообщает, каким является статус файла по сравнению с предыдущим входом в систему: «Создан», «Без изменений», «Изменен», «Удален». При выходе из системы осуществляется обновление базы хэш-кодов и зашифрование всех файлов пользователя.

Таким образом, все поставленные задачи были полностью решены.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Основы криптографии : учеб. пособие / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. М. : Гелиос АРФ, 2002. 480 с. : ил.

2 Салий, В. Н. Криптографические методы и средства защиты информации : учеб. пособие // СГУ – Саратовский государственный университет [Электронный ресурс] : [сайт]. URL: http://www.sgu.ru/sites/default/files/textdocsfiles/2015/11/09/saliy_v.n._kriptograficheskie_metody_i_sredstva_zashchity_informacii.pdf (дата обращения: 10.12.2015). Загл. с экрана. Яз. рус.

3 ГОСТ Р 34.11-2012 Информационная технология. Криптографическая защита информации. Функция хэширования // Федеральное агентство по техническому регулированию и метрологии [Электронный ресурс] : [сайт]. URL: http://protect.gost.ru/document.aspx?control=7&id=180209 (дата обращения: 10.12.2015). Загл. с экрана. Яз. рус.

4 Электронная подпись [Электронный ресурс] // Википедия [Электронный ресурс] : свободная энциклопедия. URL: https://ru.wikipedia.org/wiki/Электронная_подпись (дата обращения: 11.12.2015). Загл. с экрана. Яз. рус.

5 Аутентичность // Словари [Электронный ресурс] : [сайт]. URL: http://www.finam.ru/dictionary/wordf00A2B/ (дата обращения: 14.12.2015). Загл. с экрана. Яз. рус.

6 Защита данных с помощью криптографических преобразований // Московское отделение Пензенского научно-исследовательского электротехнического института [Электронный ресурс] : [сайт]. URL: http://www.security.ru/default.php?target=datasecurity (дата обращения: 14.12.2015). Загл. с экрана. Яз. рус.

7 Целостность информации // Википедия [Электронный ресурс] : свободная энциклопедия. URL: https://ru.wikipedia.org/wiki/Целостность_информации (дата обращения: 14.12.2015). Загл. с экрана. Яз. рус.

8 Контроль целостности данных // Портал электронного обучения [Электронный ресурс] : [сайт]. URL: http://tulpar.kfu.ru/mod/page/view.php?id=8394 (дата обращения: 10.12.2015). Загл. с экрана. Яз. рус.

9 SECURE HASH Алгоритмы (SHA-1, SHA-2) [Электронный ресурс] : [сайт]. URL: http://solutionmes.wikidot.com/crypto-sha (дата обращения: 14.12.2015). Загл. с экрана. Яз. рус.

10 Блочные шифры // Криптография [Электронный ресурс] : [сайт]. URL: http://kryptography.narod.ru/block.html (дата обращения: 14.12.2015). Загл. с экрана. Яз. рус.

11 Блочные шифры и их криптоанализ // Энциклопедия теоретической и прикладной криптографии [Электронный ресурс] : [сайт]. URL: http://cryptowiki.net/index.php?title=Блочные_шифры_и_их_криптоанализ (дата обращения: 14.12.2015). Загл. с экрана. Яз. рус.

12 Общее описание криптоалгоритма AES // Практическая криптология [Электронный ресурс] : [сайт]. URL: http://bit.nmu.org.ua/ua/student/metod/cryptology/лекция%209.pdf (дата обращения: 15.12.2015). Загл. с экрана. Яз. рус.

13 ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования // Электронный фонд правовой и нормативно-технической документации [Электронный ресурс] : [сайт]. URL: http://docs.cntd.ru/document/gost-28147-89 (дата обращения: 12.10.2015). Загл. с экрана. Яз. рус.

14 EF Software // EF CheckSum Manager [электронный ресурс] : [сайт]. URL: http://www.efsoftware.com/cm/e.htm (дата обращения: 07.12.2015). Загл. с экрана. Яз англ.

15 NoVirusThanks // MD5 Checksum Tool [электронный ресурс] : [сайт]. URL: http://www.novirusthanks.org/products/md5-checksum-tool/ (дата обращения: 08.12.2015). Загл. с экрана. Яз. англ.