РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 715 293**(13) **C1**

(51) МПК
G06F 21/62 (2013.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
G06F 21/6209 (2020.01); H04L 9/30 (2020.01); H04L 9/32 (2020.01)

(21)(22) Заявка: **2019121713, 11.07.2019**

(24) Дата начала отсчета срока действия патента:
11.07.2019

Дата регистрации:
26.02.2020

Приоритет(ы):
(22) Дата подачи заявки: **11.07.2019**

(45) Опубликовано: **26.02.2020** Бюл. № **6**

Адрес для переписки:
127287, Москва, Старый Петровско-Разумовский пр-д, 1/23, стр. 1, Открытое акционерное общество "Информационные технологии и коммуникационные системы"

(72) Автор(ы):
Елфимов Андрей Владимирович (RU)

(73) Патентообладатель(и):
Открытое акционерное общество "Информационные технологии и коммуникационные системы" (RU)

(56) Список документов, цитированных в отчете о поиске: **US 9460296 B2, 04.10.2016. US 6378071 B1, 23.04.2002. RU 2395166 C2, 20.07.2010. RU 2546585 C2, 10.04.2015.**

(54) Способ защиты данных в вычислительной системе

(57) Реферат:

Изобретение относится к области защиты данных. Техническим результатом является повышение защищенности от несанкционированного доступа к файлам внутри области защищенного хранения файлов. Способ защиты данных в вычислительной системе заключается в том, что формируют ключ для шифрования данных в области защищенного хранения файлов; вычисляют значение хэш-функции для ключа; формируют метаданные, содержащие значение хэш-функции; сохраняют метаданные; зашифровывают данные в файлах области защищенного хранения файлов с использованием ключа; если получают запрос пользовательского приложения, включающий ключ, на чтение данных файла из области защищенного хранения файлов, то с использованием управляющего приложения получают ключ для доступа к области защищенного хранения файлов; вычисляют значение хэш-функции для ключа; если значение хэш-функции ключа совпадает со значением хэш-функции ключа, сохраненным в метаданных, то определяют наличие доступа прикладной программы, иначе - отсутствие доступа; если у пользовательского приложения отсутствует доступ, то возвращают данные без расшифрования; если у пользовательского приложения имеется доступ, то расшифровывают данные с использованием ключа; возвращают расшифрованные данные пользовательскому приложению. 2 з.п. ф-лы.

RU 2715293 C1

RU 2715293 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 715 293**(13) **C1**

(51) Int. Cl.
G06F 21/62 (2013.01)

(12) ABSTRACT OF INVENTION

(52) CPC
G06F 21/6209 (2020.01); *H04L 9/30* (2020.01); *H04L 9/32* (2020.01)

(21)(22) Application: **2019121713, 11.07.2019**

(24) Effective date for property rights:
11.07.2019

Registration date:
26.02.2020

Priority:
(22) Date of filing: **11.07.2019**

(45) Date of publication: **26.02.2020** Bull. № **6**

Mail address:
127287, Moskva, Staryj Petrovsko-Razumovskij pr-d, 1/23, str. 1, Otkrytoe aktsionernoe obshchestvo "Informatsionnye tekhnologii i kommunikatsionnye sistemy"

(72) Inventor(s):
Elfimov Andrej Vladimirovich (RU)

(73) Proprietor(s):
Otkrytoe aktsionernoe obshchestvo "Informatsionnye tekhnologii i kommunikatsionnye sistemy" (RU)

RU 2715293 C1

(54) METHOD OF PROTECTING DATA IN A COMPUTING SYSTEM

(57) Abstract:

FIELD: data protection.

SUBSTANCE: method of protecting data in a computer system involves generating a key for encrypting data in a secure file storage area; calculating a key hash value; generating metadata containing hash function value; storing metadata; encrypting data in files of secure file storage area using key; if a user application request is received, including a key, to read file data from the secure file storage area, then using the control application, obtaining a key for accessing the secure storage area of files; calculating a key hash value; if key hash function value is equal to key hash function value stored in metadata, then availability of application access is determined, otherwise – absence of access; if user application does not have access, data is returned without decryption; if the user application has access, then decrypting the data using the key; returning the decrypted data to the user application.

EFFECT: improved protection against unauthorized access to files inside the protected file storage area.

3 cl

RU 2715293 C1

Область техники, к которой относится изобретение

Предлагаемое изобретение относится к вычислительной технике и, в частности, к области защиты данных путем шифрования и может быть использовано для контроля доступа к файлам, содержащим конфиденциальную информацию и хранящимся в области защищенного хранения.

Уровень техники

Для обеспечения защиты данных в информационных и вычислительных системах, в том числе сетевых, используют шифрование данных и доступ к ним на основе ключа шифрования.

Так, известен способ предоставления доступа к зашифрованному контенту заданной одной из множества абонентских систем (патент РФ №2395166, приоритет от 30.07.2004 г.), причем

каждая из этого множества абонентских систем выполнена с возможностью получать пакет защищенного контента, включающий в себя зашифрованный контент и указание местоположения, из которого должен запрашиваться объект данных прав,

причем эта заданная одна из упомянутого множества абонентских систем дополнительно включает в себя по меньшей мере одно устройство, имеющее доступ к таким образом полученному пакету защищенного контента и снабженное функцией агента, предоставляющей ему возможность извлекать объект данных прав из модуля средства выдачи прав, выдающего объекты данных прав,

причем эти объекты прав выдаются из указанного местоположения и предоставляют упомянутому по меньшей мере одному устройству доступ к, по меньшей мере, части зашифрованного контента,

при этом объект данных прав включает в себя, по меньшей мере, информацию ключа контента, позволяющую дешифровать, по меньшей мере, часть зашифрованного контента,

причем объект данных прав криптографически привязан к упомянутому по меньшей мере одному устройству, так что только это, по меньшей мере одно устройство, которое включает в себя функцию агента и к которому объект данных прав был привязан, способно получать информацию ключа контента, при этом способ содержит этапы, на которых

- переносят модуль средства выдачи прав в защищенную среду устройства обработки защищенных данных, причем это устройство обработки защищенных данных предназначено для включения в упомянутую заданную одну из упомянутого множества абонентских систем и при его работе в этой заданной одной из упомянутого множества абонентских систем
- принимают в модуле средства выдачи прав запрос на объект данных прав и
- формируют объект данных прав, криптографически привязанный к упомянутому по меньшей мере одному устройству, при этом модуль средства выдачи прав, представляющий собой исполняемый процессором модуль компьютерной программы, обеспечивает при своей работе устройству обработки защищенных данных возможность формировать объект данных прав, который криптографически привязан к упомянутому по меньшей мере одному устройству.

Способ ориентирован на использование в сети, в частности, в сети сотовой связи, с большим количеством абонентов.

Однако, известный способ имеет ряд недостатков, среди которых отсутствие возможности проведения резервного копирования данных без расшифрования, отсутствие какой-либо контроля пользователя над зашифрованными данными,

отсутствие возможности изменения зашифрованных данных.

Известен также способ для избирательного расшифрования файлов, содержащих конфиденциальную информацию (патент США №9460296, приоритет от 19.07.2013 г.).

Этот способ состоит в контроле над областью защищенного хранения файлов, включающей как минимум один файл, с использованием процесса избирательного расшифрования, ассоциированного с этой областью, в которой содержимое как минимум одного файла защищено шифрованием, обнаружении запроса прикладной программы на доступ, как минимум, к одному файлу, определении какое приложение требует доступа, как минимум, к части содержимого запрашиваемого файла, при определении того, что приложению запрещен доступ к содержимому файла, разрешении прикладной программе в доступе к содержимому файла без расшифрования содержимого, при определении того, что приложению разрешен доступ к содержимому файла: расшифровании содержимого файла, тем самым разрешая приложению доступ к расшифрованному содержимому файла, при обнаружении запроса на запись от прикладной программы в файл, не находящийся в области защищенного хранения файлов, обратном зашифровании содержимого файла, используя процесс избирательного шифрования, перед записью в незащищенное место, т.е. повторном зашифровании расшифрованного содержимого файла, скрытно от прикладного приложения, где областью защищенного хранения файлов является папка файловой системы.

Описанный способ принят за прототип.

Основным недостатком известного способа является то, что защита данных привязывается не к криптографическому ключу, а к типу прикладной программы, требующей ввода/вывода данных в защищенное хранилище.

Кроме того, отсутствие доступа напрямую к зашифрованной информации в обход процесса избирательного шифрования ограничивает возможности по резервному копированию данных без раскрытия защищаемых данных.

При отсутствии хранения метаданных, необходимых для шифрования/расшифрования файлов, в известном способе серьезно ограничиваются возможности применения современных подходов к шифрованию блочных данных и повышается нагрузка на ключи шифрования, используемые в криптографических операциях с файлами.

Раскрытие изобретения

Техническим результатом является

1) повышение защищенности от несанкционированного доступа к файлам внутри области защищенного хранения файлов,

2) обеспечение возможности проведения резервного копирования защищенных данных без их расшифрования.

Для этого предлагается способ защиты данных в вычислительной системе, содержащей

- операционную систему;
- область защищенного хранения файлов;
- управляющее приложение, выполненное с возможностью
  - управления доступом к области защищенного хранения файлов;
  - формирования ключа шифрования для области защищенного хранения файлов;
  - зашифрования и расшифрования данных с использованием ключа;
  - хранения ключа;
- пользовательские приложения, выполненные с возможностью
  - доступа к области защищенного хранения файлов;

- получения и передачи ключа для доступа к области защищенного хранения файлов;

способ, заключающийся в том, что

- формируют ключ для шифрования данных в области защищенного хранения файлов;
- вычисляют значение хэш-функции для ключа;
- формируют метаданные, содержащие значение хэш-функции;
- сохраняют метаданные;
- зашифровывают данные в файлах области защищенного хранения файлов с использованием ключа;
- при необходимости, посылают запрос пользовательского приложения, включающий ключ, на чтение из области защищенного хранения файлов;
- если получают запрос пользовательского приложения, включающий ключ, на чтение данных файла из области защищенного хранения файлов, то с использованием управляющего приложения
  - получают ключ для доступа к области защищенного хранения файлов;
  - вычисляют значение хэш-функции для ключа, полученного вместе с запросом;
  - если значение хэш-функции ключа, полученного вместе с запросом, совпадает со значением хэш-функции ключа, сохраненным в метаданных, то определяют наличие доступа прикладной программы, иначе - отсутствие доступа;
  - если у пользовательского приложения отсутствует доступ, то возвращают данные без расшифрования;
  - если у пользовательского приложения имеется доступ, то
    - расшифровывают данные с использованием ключа;
    - возвращают расшифрованные данные пользовательскому приложению;
- при необходимости, посылают запрос пользовательского приложения, включающий ключ, на запись в область защищенного хранения файлов,
- если получают запрос пользовательского приложения, включающий ключ, на чтение данных файла из области защищенного хранения файлов, то с использованием управляющего приложения
  - получают ключ для доступа к области защищенного хранения файлов;
  - вычисляют значение хэш-функции для ключа, полученного вместе с запросом;
  - если значение хэш-функции ключа, полученного вместе с запросом, совпадает со значением хэш-функции ключа, сохраненным в метаданных, то определяют наличие доступа прикладной программы, иначе - отсутствие доступа;
  - если у пользовательского приложения отсутствует доступ, то возвращают в пользовательское приложение сообщение об ошибке записи;
  - если у пользовательского приложения имеется доступ, то
    - зашифровывают данные с использованием ключа;
    - записывают зашифрованные данные в файл.

Сущность предлагаемого способа заключается в следующем.

В вычислительной системе, в качестве которой в самом простом случае может быть использован одиночный компьютер, создается область защищенного хранения файлов (ОЗХФ), являющаяся папкой файловой системы. Далее, на этом же компьютере, запускается управляющее приложение (УП). Этому приложению устанавливается в соответствие созданная ранее ОЗХФ. Далее УП реализует перехват запросов ввода/вывода пользовательских приложений к файловой системе, имеющих целью файлы

внутри ОЗХФ. Затем в УП регистрируется пользователь, УП формирует для этого пользователя ключ, возвращает этот ключ пользователю, вычисляет значение хэш-функции для ключа, формирует метаданные, связанные с ОЗХФ, записывает значение хэш-функции в метаданные, сохраняет метаданные в ОЗХФ.

При перехвате запроса на чтение или запись в файл ОЗХФ, УП получает ключ К1, ассоциированный с пользователем, для манипуляций с данными этого файла из следующих источников: из внутреннего хранилища УП, где ключ ассоциирован с учетной записью пользователя в операционной системе (ОС); ключ К1 запрашивается УП непосредственно у пользователя при доступе к данным; ключ К1 запрашивается у пользователя при старте системы.

При чтении данных, УП считывает метаданные из ОЗХФ, извлекает из метаданных значение хэш-функции ключа, сравнивает это значение с результатом хэш-функции от ключа К1. Если результаты хэш-функций не совпадают, УП предоставляет запрошенные запросом ввода/вывода данные без расшифрования. Иначе, УП расшифровывает запрашиваемые данные на ключе К1 и возвращает в запрос ввода/вывода расшифрованные данные.

При записи данных, УП завершает запрос ввода-вывода на запись с ошибкой, если результат хэш-функции ключа К1 не совпадает с результатом хэш-функции ключа, использованного при зашифровании; иначе, данные при записи зашифровываются на предоставленном ключе К1. При записи данных нового файла, эти данные, с помощью УП, зашифровываются на предоставленном ключе и сохраняются в ОЗХФ, результат хэш-функции этого ключа сохраняется в метаданных.

Кроме того, при запуске УП возможно создание папки в файловой системе, представляющей ОЗХФ без перехвата запросов ввода/вывода, то есть только с зашифрованным содержимым ОЗХФ. При копировании файлов в/из этого места появляется возможность архивации/обмена защищенными данными без раскрытия расшифрованных данных.

Метаданные, которые добавляются к файлам внутри ОЗХФ, могут храниться, например, в виде отдельного файла метаданных в ОЗХФ, либо внутри каждого зашифрованного защищенного файла в структуре файлов ОЗХФ.

Метаданные могут включать в себя одну или несколько следующих структур данных:

- значение хэш-функции ключа, использованного при создании файла, для аутентификации доступа;
- зашифрованные вспомогательные ключи для каждого блока (части) файла, ассоциированного с метаданными, для снижения количества использований основного ключа шифрования;
- вспомогательные данные ключа, использующегося для доступа к файлу, для контроля целостности ключа, контроля использований и для любых возможных вспомогательных преобразований ключа;
- информацию, используемую для контроля целостности данных, ассоциированных с метаданными.

Дополнительная возможность защиты возникает при использовании предложенного способа при разделении файлов внутри ОЗХФ на части с ассоциацией каждой части своего ключа шифрования и метаданных.

При чтении данных, в этом случае, УП считывает метаданные из ОЗХФ, извлекает из метаданных значение хэш-функции ключа, сравнивает это значение с результатом хэш-функции от ключа К1. Если результаты хэш-функций не совпадают, УП предоставляет запрошенные запросом ввода/вывода данные без расшифрования. Иначе,

УП определяет часть файла, к которой осуществляется доступ, считывает метаданные для этой части, вычисляет и расшифровывает на ключе К1 из этих метаданных ключ шифрования данных части (К2), расшифровывает запрашиваемые данные части файла на ключе К2 и возвращает в запрос ввода/вывода расшифрованные данные.

При записи данных, в случае работы с частями файлов, УП завершает запрос ввода-вывода на запись с ошибкой, если результат хэш-функции ключа К1 не совпадает с результатом хэш-функции ключа, использованного при зашифровании; иначе, УП определяет часть файла, к которой осуществляется доступ, считывает метаданные для этой части, вычисляет и расшифровывает на ключе К1 из метаданных ключ шифрования данных части (К2), либо заново формирует его, если для этой части еще не производилось операций ввода-вывода, данные при записи зашифровываются на ключе К2.

Таким образом, предложенный способ позволяет повысить защищенность от несанкционированного доступа к файлам внутри области защищенного хранения файлов и предоставить возможность проведения резервного копирования защищенных данных без их расшифрования.

Осуществление изобретения

Реализация предложенного способа может быть осуществлена в вычислительной системе, работающих под управлением ОС, например, Solaris, Android и др.

Предпочтительный вариант реализации изобретения: программное решение процесса избирательного расшифрования в операционных системах Windows/Linux. В Windows системах реализация УП может быть произведена в виде драйвера фильтра файловой системы с комплектом прикладного ПО для администрирования и настройки.

В Linux системах реализация УП может быть произведена в виде системного приложения с использованием технологии FUSE (Filesystem in Userspace) с аналогичным комплектом прикладного ПО для администрирования и настройки.

Рассмотрим осуществление способа на примере ОС Linux Debian 9.

Для подготовки к использованию предлагаемого способа необходимо сформировать УП в виде программного средства. Это средство представляет собой программу, которую, зная ее назначение и выполняемые функции, может сформировать специалист в области программирования (программист). Подготовленное средство после сформирования устанавливается (инсталлируется) в вычислительную систему.

Затем вычислительная система начинает работу в обычном режиме. В ходе ее работы:

- получают у администратора системы путь к ОЗХФ;
- запускают УП и, при его работе, с использованием технологии FUSE, формируют папку файловой системы, содержащую, во-первых, папку со представлением файлов в ОЗХФ и, во-вторых, папку с зашифрованными данными и метаданными; доступ во вторую папку с зашифрованными данными и метаданными со стороны УП не ограничивается;
- при обращении пользовательских программ к файлам внутри папки файловой системы, с представлением файлов ОЗХФ, средствами технологии FUSE обеспечивается перехват запросов ввода/вывода к файлам;
- УП формирует ключ К1 одним из следующих способов: либо функцией формирования ключевой информации из парольной фразы, запрошенной у пользователя, либо непосредственной выработкой из одного из имеющихся в системе источников энтропии, и, если отсутствует возможность повторной выработки, сохраняется во внутреннем хранилище УП, иначе не сохраняется, а запрашивается у пользователя.
- УП получает ключ К1 для работы с данными одним из следующих способов: из

внутреннего хранилища УП, где ключ ассоциирован с учетной записью пользователя в ОС; ключ К1 запрашивается УП непосредственно у пользователя при доступе к данным; ключ К1 запрашивается у пользователя при старте системы;

- УП осуществляет действия по шифрованию/расшифрованию данных из ОЗХФ в соответствии с результатом аутентификации по ключу К1 и возвращает эти данные в перехваченный запрос ввода/вывода, при этом выполняя чтение или запись в папку с зашифрованными данными и метаданными.

После завершения работы с ОЗХФ процесс УП завершается, полностью ограничивая доступ к открытым данным ОЗХФ.

При необходимости

- ограничения количества информации, обрабатываемой на одном ключе,
- частого обращения к части файла защищаемой информации,
- контроля части защищаемого файла,
- смены ключа шифрования файла без смены ключа доступа,

возможна реализация предложенного способа для файлов из ОЗХФ, логически разделенных на части.

В ходе работы вычислительной системы:

- получают у администратора системы путь к ОЗХФ;
- запускают УП и, при его работе с использованием технологии FUSE, формируют папку файловой системы, содержащую, во-первых, папку со представлением файлов в ОЗХФ и, во-вторых, папку с зашифрованными данными и метаданными; доступ во вторую папку с зашифрованными данными и метаданными со стороны УП не ограничивается;
- при обращении пользовательских программ к файлам внутри папки файловой системы, с представлением файлов ОЗХФ, средствами технологии FUSE обеспечивается перехват запросов ввода/вывода к файлам;
- УП формирует ключ К1 одним из следующих способов: либо функцией формирования ключевой информации из парольной фразы, запрошенной у пользователя, либо непосредственной выработкой из одного из имеющихся в системе источников энтропии, и, если отсутствует возможность повторной выработки, сохраняется во внутреннем хранилище УП, иначе не сохраняется, а запрашивается у пользователя;
- УП получает ключ К1 для работы с данными одним из следующих способов: из внутреннего хранилища УП, где ключ ассоциирован с учетной записью пользователя в ОС; ключ К1 запрашивается УП непосредственно у пользователя при доступе к данным; ключ К1 запрашивается у пользователя при старте системы;
- УП при положительном результате аутентификации по ключу К1 определяет часть файла ОЗХФ, к которой выполняется запрос ввода/вывода, и получает из ОЗХФ метаданные, соответствующие этой части;
- из метаданных получают зашифрованный ключ шифрования части данных (К2) и расшифровывается на ключе К1;
- с использованием ключа К2 с использованием УП расшифровываются/зашифровываются данные запроса ввода/вывода и возвращаются в перехваченный запрос ввода/вывода, при этом УП выполняет чтение или запись в папку с зашифрованными данными и метаданными;
- при необходимости, ключ К2 меняется с помощью УП, часть данных, зашифрованная на нем перешифровывается на новом ключе и сохраняется в ОЗХФ, новый ключ сохраняется в метаданных, связанных с этой частью, зашифрованным на ключе К1.

После завершения работы с ОЗХФ процесс УП завершается, полностью ограничивая доступ к открытым данным ОЗХФ.

(57) Формула изобретения

Способ защиты данных в вычислительной системе, содержащей:

операционную систему;

область защищенного хранения файлов;

управляющее приложение, выполненное с возможностью:

управления доступом к области защищенного хранения файлов;

формирования ключа шифрования для области защищенного хранения файлов;

зашифрования и расшифрования данных с использованием ключа;

хранения ключа;

пользовательские приложения, выполненные с возможностью:

доступа к области защищенного хранения файлов;

получения и передачи ключа для доступа к области защищенного хранения файлов;

способ, заключающийся в том, что

формируют ключ для шифрования данных в области защищенного хранения файлов;

вычисляют значение хэш-функции для ключа;

формируют метаданные, содержащие значение хэш-функции;

сохраняют метаданные;

зашифровывают данные в файлах области защищенного хранения файлов с использованием ключа;

при необходимости, посылают запрос пользовательского приложения, включающий ключ, на чтение из области защищенного хранения файлов;

если получают запрос пользовательского приложения, включающий ключ, на чтение данных файла из области защищенного хранения файлов, то с использованием управляющего приложения

получают ключ для доступа к области защищенного хранения файлов;

вычисляют значение хэш-функции для ключа, полученного вместе с запросом;

если значение хэш-функции ключа, полученного вместе с запросом, совпадает со значением хэш-функции ключа, сохраненным в метаданных, то определяют наличие доступа прикладной программы, иначе - отсутствие доступа;

если у пользовательского приложения отсутствует доступ, то возвращают данные без расшифрования;

если у пользовательского приложения имеется доступ, то расшифровывают данные с использованием ключа;

возвращают расшифрованные данные пользовательскому приложению;

при необходимости, посылают запрос пользовательского приложения, включающий ключ, на запись в область защищенного хранения файлов; если получают запрос пользовательского приложения, включающий ключ, на чтение данных файла из области защищенного хранения файлов, то с использованием управляющего приложения

получают ключ для доступа к области защищенного хранения файлов;

вычисляют значение хэш-функции для ключа, полученного вместе с запросом;

если значение хэш-функции ключа, полученного вместе с запросом, совпадает со значением хэш-функции ключа, сохраненным в метаданных, то определяют наличие доступа прикладной программы, иначе - отсутствие доступа;

если у пользовательского приложения отсутствует доступ, то возвращают в пользовательское приложение сообщение об ошибке записи;

если у пользовательского приложения имеется доступ, то

зашифровывают данные с использованием ключа;

записывают зашифрованные данные в файл.

2. Способ по п. 1, в котором доступ к области защищенного хранения файлов организуется в обход процесса избирательного шифрования/расшифрования путем предоставления зашифрованного содержимого области защищенного хранения файлов как папки в файловой системе.

3. Способ по п. 1, в котором зашифрованные файлы из области защищенного хранения файлов логически разделены на части, причем каждой части файла устанавливается в соответствие ключ доступа, на котором шифруется эта часть, а в состав метаданных для соответствующей части файла включают ключ доступа, зашифрованный на ключе шифрования для всего файла.