РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 506 704** (13) **C2**

(51) МПК
H04L 12/24 (2006.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2011106126/07, 17.07.2009**

(24) Дата начала отсчета срока действия патента:
17.07.2009

Приоритет(ы):
(30) Конвенционный приоритет:
18.07.2008 US 61/082,130

(43) Дата публикации заявки: **27.08.2012** Бюл. № 24

(45) Опубликовано: **10.02.2014** Бюл. № 4

(56) Список документов, цитированных в отчете о поиске: **US 2004106415 A1, 03.06.2004. WO 2006086505 A2, 17.08.2006. RU 2322766 C2, 20.04.2008. Y. Sun и др., An Architecture and Key Management Approach for Maintaining Privacy in Location Based Group Services, 26.07.2006,. http: //www.cse.psu.edu/~tlp/paper/LBS-2-6-06.pdf.**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **18.02.2011**

(86) Заявка PCT:
CA 2009/001028 (17.07.2009)

(87) Публикация заявки PCT:
WO 2010/006450 (21.01.2010)

Адрес для переписки:
129090, Москва, ул.Б.Спасская, 25, стр.3, ООО "Юридическая фирма Городисский и Партнеры", пат.пов. А.В.Мицу, рег.№ 364

(72) Автор(ы):
МАККАРТИ Чад Чарльз (CA),
ЛАВЛЭНД Дамьен Дж. (CA),
ВИБЕ Тревор (CA)

(73) Патентообладатель(и):
ЭБСОЛЮТ СОФТВЭАР КОРПОРЕЙШН (CA)

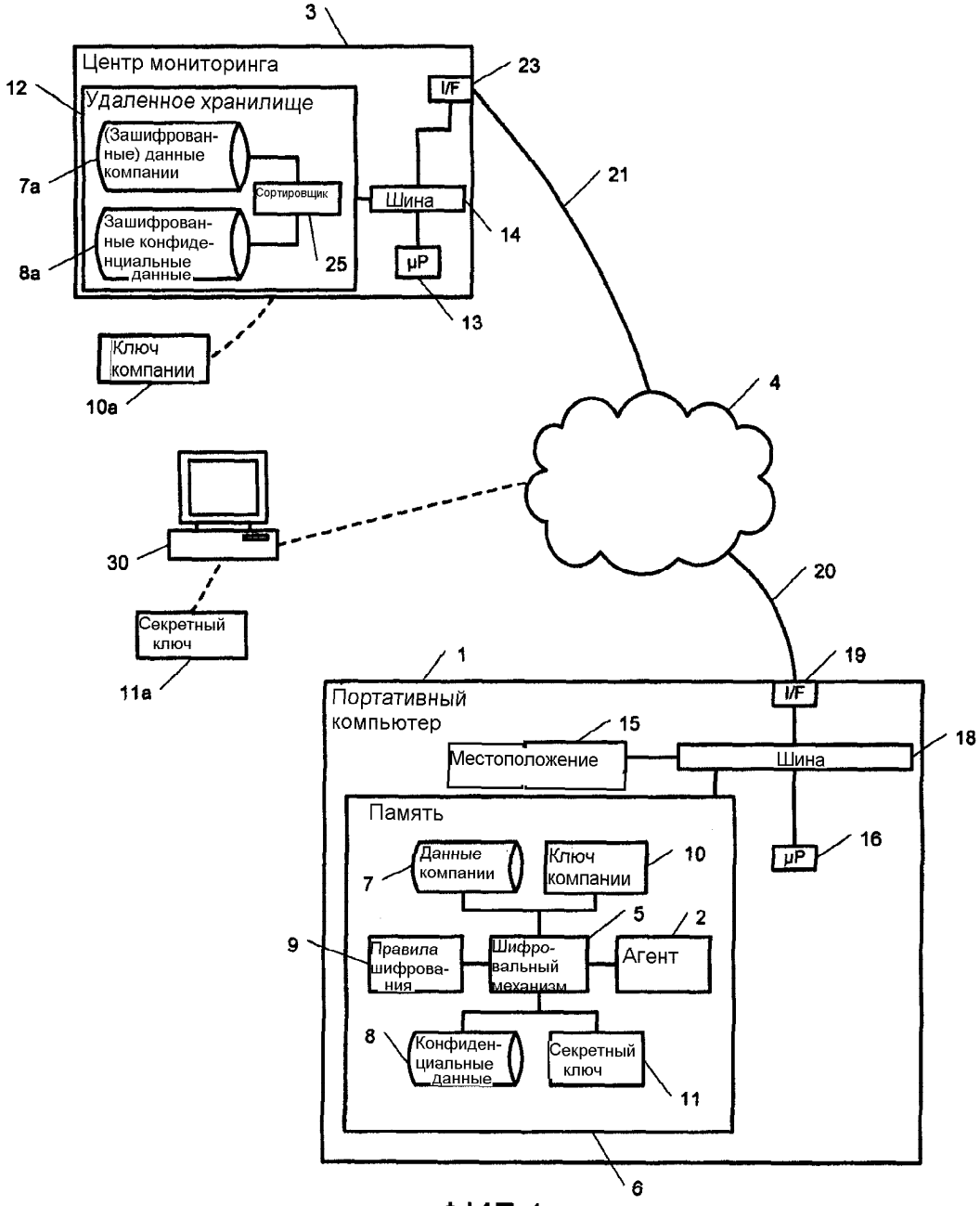
RU 2506704 C2

RU 2506704 C2

(54) УПРАВЛЕНИЕ КОНФИДЕНЦИАЛЬНОСТЬЮ ДЛЯ ОТСЛЕЖИВАЕМЫХ УСТРОЙСТВ

(57) Реферат:

Изобретение относится к системам защиты данных. Технический результат заключается в повышении эффективности защиты данных. Устройство, способ, система и компьютерно-читаемый носитель для защиты конфиденциальных данных, в то же время позволяющие мониторинг или отслеживание электронных устройств, которые совместно используются для коммерческих и конфиденциальных целей, посредством условного шифрования данных, передающихся от устройства, которое отслеживается, к компьютеру в удаленном местоположении, при этом передача данных может быть предназначена для отслеживания, мониторинга, резервного копирования данных или для возврата в случае потери или кражи. 3 н. и 12 з.п. ф-лы, 5 ил.



ФИГ.1

RU 2506704 C2

RU 2506704 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 506 704** (13) **C2**

(51) Int. Cl.
H04L 12/24 (2006.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2011106126/07, 17.07.2009**

(24) Effective date for property rights:
17.07.2009

Priority:
(30) Convention priority:
18.07.2008 US 61/082,130

(43) Application published: **27.08.2012** Bull. 24

(45) Date of publication: **10.02.2014 Bull. 4**

(85) Commencement of national phase: **18.02.2011**

(86) PCT application:
CA 2009/001028 (17.07.2009)

(87) PCT publication:
WO 2010/006450 (21.01.2010)

Mail address:
129090, Moskva, ul.B.Spasskaja, 25, str.3, OOO "Juridicheskaja firma Gorodisskij i Partnery", pat.pov. A.V.Mitsu, reg.№ 364

(72) Inventor(s):
MAKKARTI Chad Charl'z (CA),
LAVLEhND Dam'en Dzh. (CA),
VIBE Trevor (CA)

(73) Proprietor(s):
EhBSOLJuT SOFTVEhAR KORPOREJShN (CA)

RU 2506704 C2

(54) MANAGING CONFIDENTIALITY FOR MONITORED DEVICES

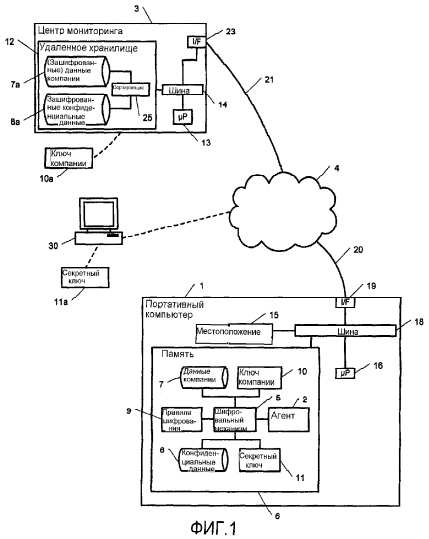
(57) Abstract:

FIELD: radio engineering, communication.

SUBSTANCE: invention relates to data security systems. The apparatus, method, system and computer-readable medium for protecting confidential data also enable to monitor or track electronic devices which are shared for commercial and confidential purposes, through arbitrary encryption of data transmitted from the device being monitored to a computer at a remote location, wherein data transmission can be intended for tracking, monitoring, back up of data or for return in case of loss or storage.

EFFECT: high efficiency of data protection.

15 cl, 5 dwg



ФИГ.1

RU 2506704 C2

УРОВЕНЬ ТЕХНИКИ

Настоящее раскрытие относится к защите конфиденциальности пользователей, в то же время предоставляя возможность отслеживания электронных устройств.

Портативные компьютеры и все в большей степени другие электронные устройства, такие как сотовые телефоны, персональные цифровые секретари (PDA), интеллектуальные телефоны (например, BlackBerry™, iPhone™), карты памяти, персональные медиа устройства (например iPod™), игровые устройства и персональные компьютеры, отслеживаются удаленно, так чтобы их можно было вернуть в случае кражи. Такое отслеживание может быть осуществлено посредством отправки информации о местоположении удаленному месту хранения или почтовому серверу.

Информация о праве собственности, как положено, хранится на электронных устройствах, таких как персональные компьютеры, портативные компьютеры или персональные цифровые ассистенты, и необходимость защиты такого права собственности или критичных данных, и возврата таких устройств, если они были утеряны или украдены, самоочевидна. Однако при обеспечении защиты таких устройств и/или данных необходимо принимать во внимание и конфиденциальность пользователей таких устройств.

СУЩНОСТЬ ИЗОБРЕТЕНИЯ

Данная сущность не является исчерпывающим обзором, направленным на установление границ предмета изобретения, который описан и заявлен в материалах настоящей заявки. Сущность представляет аспекты предмета изобретения в упрощенной форме для обеспечения их базового понимания в качестве вступления к подробному описанию, которое представлено далее.

Во многих случаях работодатель захочет отследить все портативные компьютеры (или другие электронные устройства), которые выданы его служащим. По причинам конфиденциальности, некоторые служащие могут быть против отслеживания 24/7 портативного компьютера, так как персональное местоположение и сбор исторических персональных местоположений считается конфиденциальной информацией. Это особо важно в случае, если работодатель дал служащему разрешение на персональное использование ноутбука в нерабочее время. Существует интерес, осуществляется ли мониторинг работодателем, или мониторинг осуществляет неродственная третья сторона, такая как охранная компания.

Предмет изобретения, описанный в материалах настоящей заявки, обеспечивает систему и способ условного шифрования данных, передаваемых от устройства, которое отслеживается, к компьютеру в удаленном местоположении. Передача данных может применяться для отслеживания, для целей мониторинга, резервного копирования данных или для возврата в случае потери или кражи.

В одном из вариантов осуществления существует несколько аспектов шифрования. Для предотвращения несанкционированного доступа, конфиденциальные данные шифруются перед их передачей к удаленному местоположению, и не могут быть расшифрованы без секретного ключа. Будут ли данные зашифрованы или нет перед передачей к удаленному местоположению, может зависеть от того, являются ли они конфиденциальными или коммерческими данными, определение чего может зависеть от некоторых условий. Условия могут быть временными, такими, что для данных, созданных в течение некоторых часов дня (таких как рабочие часы), данные считаются относящимися к работе, и не шифруются перед передачей, или предварительно шифруются, и могут быть расшифрованы в удаленном месте,

используя ключ расшифровки, относящийся к работе. Для данных, созданных в другие часы, такие как нерабочие часы, данные могут считаться конфиденциальными и шифроваться перед передачей. В предпочтительном варианте осуществления конфиденциальные данные могут быть расшифрованы только с согласия пользователя данного устройства, используя секретный ключ расшифровки.

Передаваемые данные обычно являются информацией о местоположении или информацией, относящейся к местоположению, такой как адреса интернет протокола (IP), координаты GPS (системы глобального позиционирования), мощности сигнала Wi-Fi, мощности сигнала вышки сотовой связи, времена в данных местоположениях, время, проведенное в этих местоположениях, и индикация опознавательных знаков для устройства, но также могут включать в себя посещенные веб-сайты, нажатия на клавиши, электронные сообщения, версии программного обеспечения, запуск программного обеспечения, спецификации устройства, движения мыши и файлы или подробности созданных, удаленных, скопированных, переданных, открытых, отмеченных, выбранных и/или измененных файлов. Однако, как будет легко понятно специалистам в данной области техники, раскрытый предмет изобретения может в равной степени применяться для защиты других конфиденциальных данных, созданных, используя устройство для совместного конфиденциального и коммерческого использования, либо совместно с информацией о местоположении или информацией, относящейся к местоположению, либо отдельно. Другие конфиденциальные данные, которые могут быть защищены, включают в себя, например, данные использования, посещенные веб-сайты, проигрываемые видео- и аудиофайлы, загрузки, нажатия клавиш, моментальные снимки экранов, электронные письма, файлы и другие конфиденциальные данные.

ОПИСАНИЕ ЧЕРТЕЖЕЙ

Для более полного понимания природы и преимуществ раскрытого предмета изобретения, а также предпочтительного режима его использования, должны быть сделаны ссылки на последующее подробное описание, читаемое в сочетании с сопроводительными чертежами. На чертежах подобные ссылочные числа обозначают подобные или схожие этапы или части.

Фиг.1 является схематической функциональной блок-схемой системы и способа условного шифрования данных в соответствии с вариантом осуществления раскрытого предмета изобретения, встроенных в портативный компьютер.

Фиг.2 является функциональной схемой последовательности операций, схематически представляющей осуществляемую после кражи последовательность выполняемых действий системы и способа условного шифрования данных в соответствии с вариантами осуществления раскрытого предмета изобретения.

Фиг.3 является функциональной схемой последовательности операций, схематически представляющей процесс шифрования системы и способа условного шифрования данных в соответствии с вариантами осуществления раскрытого предмета изобретения.

Фиг.4 является функциональной схемой последовательности операций, схематически представляющей процесс шифрования системы и способа условного шифрования данных в соответствии с альтернативными вариантами осуществления раскрытого предмета изобретения.

Фиг.5 является функциональной схемой последовательности операций, схематически представляющей процесс шифрования системы и способа условного шифрования данных в соответствии с дополнительными альтернативными

вариантами осуществления раскрытого предмета изобретения.

ПОДРОБНОЕ ОПИСАНИЕ КОНКРЕТНЫХ ВАРИАНТОВ ОСУЩЕСТВЛЕНИЯ

А. Терминология

Агент, в качестве используемого в материалах настоящей заявки, - это агент программного обеспечения, аппаратного обеспечения или программно-аппаратного обеспечения, который в идеале является постоянным и незаметным, и который постоянно хранится в компьютере или другом электронном устройстве. Агент предпочтительно обеспечивает обслуживающие функциональные назначения, которые требуют связь с удаленным сервером. Агент устойчив к повреждениям и может иметь возможность поддержки и/или обеспечения различных служб, таких как удаление данных, защита с помощью межсетевого экрана, шифрование данных, отслеживание местоположения, уведомление сообщениями, и оснащение и обновления программного обеспечения. Иллюстративный вариант осуществления агента найден в коммерчески доступном продукте Computrace Agent™. Технология, лежащая в основе Computrace Agent™, была раскрыта и запатентована в США и других странах, патенты которых в большинстве случаев были переуступлены Absolute Software Corporation. Смотрите, например, патенты US № 5715174; 5764892; 5802280; 6244758; 6269392; 6300863; и 6507914, и родственные иностранные патенты. Подробности постоянных функциональных назначений агента раскрыты в публикациях заявок на выдачу патента США № US 2005/0216757 и US 2006/0272020. Технические раскрытия этих документов полностью включены в материалы настоящего описания посредством ссылки, как если бы были полностью в ней изложены. Возможно использовать агент, эквивалентный Computrace Agent™, или, менее предпочтительно, альтернативный агент с меньшей функциональностью. Для целей настоящего раскрытия минимальным функциональным признаком агента является способствование осуществлению связи между электронным устройством и центром мониторинга. Осуществления связи могут быть инициированы агентом, центром мониторинга или обоими.

Хост - это электронное устройство, подлежащее защите, которое типично предназначено для совместного коммерческого и конфиденциального использования. Примеры хостов включают в себя портативный компьютер, компактный компьютер или интеллектуальный телефон. Агент постоянно хранится в хосте.

Центр мониторинга - это охранный сервер или другой компьютер или сервер, с которым связывается агент или которому отправляет сообщение. Это может быть почтовый сервер или может быть распределение серверов или других компьютеров. Например, при условии, что хосту доступно Интернет соединение, агент может вызвать центр мониторинга в некоторый выбранный подходящий интервал, чтобы сообщить местоположение хоста, загрузить обновления программного обеспечения, если таковые имеются, и восстановить любые модули безопасности, которые установлены или должны быть установлены на хосте. В вариантах осуществления, раскрытых в материалах настоящей заявки, агент загрузит в удаленное место хранения, расположенное в центре мониторинга, информацию о местоположении и/или любые другие данные, требуемые для передачи. Связь с центром мониторинга может иметь место, например, посредством проводной или беспроводной телефонной сети, WIFI, WIMAX, кабеля или спутника.

Шифрование - Обычно предполагается, что любые данные, которые передаются между удаленными устройствами, такими как хост и центр мониторинга, шифруются во время передачи. Однако, в настоящем документе, если контекст не требует

обратного, термин шифрование в целом относится к условному уровню шифрования, который может быть конфиденциальным шифрованием или коммерческим шифрованием, а не к типичному шифрованию, применяемому во время передачи. Более того, термин «шифрование» в материалах настоящей заявки преимущественно применяется к конфиденциальным данным (включая информацию о конфиденциальном местоположении и/или любые другие конфиденциальные данные, требуемые для передачи), которые передаются и остаются зашифрованными и их невозможно расшифровать на удаленном центре хранения, если не предоставлен секретный ключ расшифровки. Термин «шифрование» также относится к пользователю устройства хоста, который является обладателем конфиденциальных данных, имеющему возможность управлять, будут ли шифроваться конфиденциальные данные, когда они передаются или копируются на удаленное место хранения. Конфиденциальные данные могут также относиться к персональным данным. Коммерческие данные могут также относиться к корпоративным данным, данным компании или не персональным данным.

Подробные описания представлены в основном терминами способов или процессов, символических представлений операций, функциональных возможностей и признаков изобретения. Эти описания способа и представления являются средствами, используемыми специалистами в данной области техники для наиболее эффективной передачи сущности их работ другим специалистам в данной области техники. Способ или процесс, реализуемый программным обеспечением, здесь и в целом, задуман являющимся самосогласованной последовательностью этапов, ведущей к желаемому результату. Эти этапы включают в себя физические манипуляции физическими величинами. Часто, но не обязательно, эти величины приобретают форму электрических или магнитных сигналов, пригодных для хранения, передачи, объединения, сравнения и манипулирования иным образом. В дальнейшем будет принято во внимание, что грань между аппаратным обеспечением, программным обеспечением и программно-аппаратным обеспечением не всегда четкая, специалистам в данной области техники понятно, что процессы, реализуемые программным обеспечением, могут быть осуществлены в аппаратном обеспечении, программно-аппаратном обеспечении или программном обеспечении в форме кодированных команд, таких как микрокод и/или хранимые программные команды. В общем, если не оговорено обратное, единичные элементы могут быть во множественном числе и наоборот, без потери общности. Использование мужского рода может относиться к мужскому, женскому или обоим родам.

B. Примерный вариант осуществления

Блок-схема предпочтительного варианта осуществления показана на фиг.1. Электронное устройство 1 хоста, такое как портативный компьютер, содержит агента 2, который может регулярно, непериодично, случайно, полуслучайно и/или согласно запускам связываться с удаленным хранилищем 12 в центре 3 мониторинга посредством Интернет 4, посредством других телекоммуникационных сетей или их комбинации. Обмен сообщениями SMS (Службы коротких сообщений), например, может быть использован для всех или некоторых осуществлений связи.

Агент 2 оперативно присоединен к шифровальному механизму 5, содержащему компьютерно-читаемые команды в памяти 6, который шифрует данные 7 компании и/или конфиденциальные данные 8 для передачи, согласно правилам 9 шифрования, также хранящимся в памяти 6. Один или более шифровальных ключей, например, ключ 10 компании и секретный ключ 11, могут храниться в памяти 6 электронного

устройства 1. Память 6 может быть разделена на части и/или различные типы памяти, с тем, чтобы, например, способствовать раздельному хранению данных 7 компании и конфиденциальных данных 8 в различных хранилищах. В типичном приложении пользователь устройства 1 может создать конфиденциальную директорию или папку в памяти 6, в которой любые данные, которые идентифицируются как конфиденциальные данные 8, могут быть отделены от данных 7 компании.

Устройство 1 хоста также содержит устройство 15 определения местоположения, такое как устройство приемника GPS или A-GPS, или некоторое другое устройство, выполняющее определение местоположения. Устройство 15 определения местоположения может содержаться в памяти 6 электронного устройства 1, или оно может быть компонентом или модулем, отдельным от памяти 6, как показано на фиг.1. Может быть одно, два или более устройств 15 определения местоположения, каждое из которых работает по разным принципам или одно выступает в роли резервного для другого. Электронное устройство 1 обычно содержит устройство 16 обработки для обработки команд, содержащихся в памяти 6, и чтения/записи данных в нем и из него посредством шины 18, и интерфейса 19 к Интернет 4 или другой сети связи. Следует принять во внимание, что устройство 1, которое соединяется с Интернет 4, может в некоторых случаях рассматриваться как часть Интернет 4.

Агент 2 отправляет данные 7, 8, которые могут включать в себя информацию о местоположении, центру 3 мониторинга и/или удаленному устройству(ам) 12 хранения регулярно, непериодично, случайно, полуслучайно и/или согласно запускам. Эта передача данных между агентом 2 и центром 3 мониторинга может происходить явным образом для пользователя. Перед отправкой конфиденциальные данные о местоположении (то есть данные о местоположении, записанные или собранные в нерабочее время) в хранилище 8 конфиденциальных данных могут быть зашифрованы, а данные компании о местоположении в хранилище 7 данных компании могут остаться незашифрованными. Данные о местоположении в хранилищах 7,8 данных могут присутствовать лишь кратковременно в электронном устройстве 1.

В центре 3 мониторинга два типа данных 7a, 8a могут храниться вместе или могут храниться в отдельных базах данных после сортировки посредством сортировочного модуля 25. Например, данные 7 компании, которые не зашифрованы, могут быть отмечены как таковые в устройстве 1, или могут быть идентифицированы как таковые в центре 3 мониторинга, а затем сохранены в хранилище 7a данных. Конфиденциальные данные 8, которые зашифровываются перед отправкой, могут быть отмечены как таковые в устройстве 1, или могут быть идентифицированы как таковые в центре 3 мониторинга, а затем сохранены в хранилище 8a данных. Удаленное хранилище 12 может находиться в зданиях компании или коммерческого предприятия, которое владеет электронным устройством 1, или в здании третьих лиц - охранной компании, или оно может быть на другом компьютере или сервере, или распределено во множестве компьютеров или серверов. Если данные 7a компании, которые хранятся, не зашифрованы (не считая временного шифрования во время передачи), компания сможет иметь доступ к ним, но не сможет декодировать конфиденциальные данные 8a без предоставления доступа к секретному ключу 11a расшифровки. Возможно, что шифровальный механизм 5 шифрует как данные 7 компании, так и конфиденциальные данные 8 перед их отправкой посредством агента 2 удаленному хранилищу 12, в таком случае администратору в компании понадобится ключ 10a расшифровки компании для преобразования данных 7a в

значащий (нешифрованный) формат. В любом случае конфиденциальные данные 8, которые передаются или копируются, шифруются с использованием секретного шифровального ключа 11 или пароля, который известен только пользователю электронного устройства 1. Компания не имеет доступ к секретному шифровальному ключу 11 и не может интерпретировать данные 8a, которые являются конфиденциальными и хранятся в центре 3 мониторинга.

Центр 3 мониторинга может быть сервером, который содержит интерфейс 23 к сети 4, шину 14, посредством которой связываются компоненты, внутренние по отношению к серверу, и устройство 13 обработки для обработки компьютерно-читаемых команд в удаленном хранилище 12. Примерами команд могут быть те, которые используются для сортировки входящих данных в сортировочном модуле 25, программе, позволяющей вводить шифровальные ключи, программе, позволяющей получить доступ к данным и так далее. Также в удаленном хранилище 12 зашифрованные конфиденциальные данные 8a могут храниться, также как и данные 7a компании, которые могут шифроваться или не шифроваться. Линии связи 20, 21 между электронным устройством 1, сетью 4 и центром 3 мониторинга могут быть проводными, беспроводными или кабельными.

Если пользователь захочет получить доступ к его конфиденциальным данным 8a, например, после кражи электронного устройства 1, он может получить доступ к удаленному хранилищу 12, используя терминал 30 через Интернет 4. Данные могут быть загружены в терминал 30, и ключ расшифровки пользователя 11a может быть использован для расшифровки данных 8a. Первый пароль может быть использован для извлечения конфиденциальных данных 8a, а второй пароль или ключ 11a расшифровки может быть использован для расшифровки конфиденциальных данных 8a. Альтернативно, ключ 11a расшифровки может быть предоставлен центру 3 мониторинга для того, чтобы расшифровать конфиденциальные данные 8a.

В случае кражи или утери электронного устройства 1, фиг.2 показывает процесс, через который типично проходит пользователь. О краже 40 сообщается 42 в полицию и компанию, которая владеет электронным устройством 1, и пользователь предоставляет 44 компании ключ 11a расшифровки пользователя. Это может осуществляться посредством другого компьютера 30, подключенного к Интернет 4, или ключ может быть передан непосредственно администратору компании. Этот ключ/пароль 11a расшифровки позволит компании и/или охранной компании расшифровать 46 некоторые или все конфиденциальные данные о местоположении в хранилище данных 8a, для того чтобы она могла быть предоставлена органам правопорядка, которые затем попробуют вернуть 48 электронное устройство 1. Коммерческое предприятие, компания и/или охранная компания, администрирующая мониторинг электронного устройства 1, имеет доступ к данным 7a компании о местоположении (используя ключ 10a расшифровки компании, если данные 7a компании также были зашифрованы) и может сделать эту информацию доступной для правоохранительных органов. Это означает, что пользователь потенциально жертвует конфиденциальностью местоположения только в случае кражи, а не изо дня в день или при отсутствии кражи. В некоторых вариантах осуществления, доступ к конфиденциальным данным 8a о местоположении может быть обеспечен еще на дату и время кражи или настолько близко к ней, насколько это может быть определено, или на дату и время сообщения о краже так, что вся или большая часть конфиденциальности местоположения пользователя не подвергается риску.

В вариантах осуществления, где предоставление секретного ключа раскроет

исторические данные о местоположении или другую конфиденциальную информацию, использование сторонней охранной компании может быть предпочтительным для служащих, которые не хотят, чтобы какая-либо их конфиденциальная информация когда-либо стала доступной их работодателю.

Может существовать набор правил, посредством которых шифруются конфиденциальные данные 8. Фиг.3 показывает, что после того, как агент загрузится 49, он удостоверяется в доступности 50 шифровального механизма. Шифровальный механизм 5 затем проверяет 51 время дня и извлекает 52 правило 9 шифрования, чтобы определить 53, шифровать конфиденциальные данные 8 или нет. Только в качестве примера, простым правилом может быть то, что данные 7,8 не шифруются между 9:00 и 17:00, с понедельника по пятницу. В этом примере предполагается, что будь данные конфиденциальными по сути или относящимися к работе по своей природе, они все будут обрабатываться как данные 7 компании в рабочие часы. В рабочее время нет шифрования 55 и данные 7 компании (содержащие все данные 7,8) передаются 56 к удаленному хранилищу 12. Удаленное хранилище 12 может быть расположено в центре 3 мониторинга в зданиях, в которых работает пользователь, или может быть в другом месте. После того как данные переданы 56, процесс возвращается к началу цикла на этап 51 проверки времени, так что дополнительные данные могут передаваться время от времени, после установленной задержки или после того, как будут сформированы другие данные. Вне этого времени, то есть вне обыкновенного рабочего времени, все данные предполагаются конфиденциальными данными 8 и шифруются, используя секретный ключ 11 и/или пароль, известный только пользователю электронного устройства 1. Конфиденциальные данные 8 шифруются 54 и передаются 56 к удаленному средству 3 хранения. После того как данные переданы 56, процесс возвращается к началу цикла на этап 51 проверки времени, так что дополнительные данные могут передаваться после задержки.

В качестве исключения могут быть установлены другие периоды времени в расписании, таком как описанное выше, и могут быть сделаны поправки, например, на время отпуска. Правила, включая правила, относящиеся к периодам времени, могут быть изменены или обновлены посредством агента 2 во время осуществления связи с центром мониторинга. Например, в случае кражи, измененное правило прекратить все шифрование конфиденциальных данных может связываться посредством агента 2 с модулем 9 правил шифрования. Этот вариант осуществления может устранить необходимость для пользователя снабжать секретным ключом 11a расшифровки персонал по возврату.

Коммерческие данные или данные 7 компании могут быть зашифрованы с помощью ключа 10, известного лишь коммерческому предприятию, компании, владельцу или администратору электронного устройства 1. Альтернативно, может существовать отдельный шифровальный процесс для хранения данных компании, который происходит в удаленном месте 3 мониторинга. Таким образом, пользователь не будет иметь доступа к шифровальному ключу компании.

Применение правил 9 может в некоторых вариантах осуществления зависеть от ввода пользователем пароля. Как показано на фиг.4, после того, как электронное устройство перезагружается 60, оно просит 62 пользователя ввести пароль. Если 63 пароль введен правильно, правила 9 применяются 64, и конфиденциальные данные 8 шифруются согласно секретному шифровальному ключу 11. Если 63 пароль введен неправильно 65 или не введен, данные 8 не шифруются согласно секретному ключу 11,

потому что в этом случае либо устройство 1 было украдено, либо пользователь желает использовать устройство для задач, относящихся к работе. Зашифрованы данные или нет, они передаются 68 к удаленному хранилищу 3. После передачи 68 система возвращается к началу цикла 69 в процессе, чтобы время от времени, регулярно или как только и когда необходимо, другие данные могли быть переданы.

В альтернативном варианте осуществления данные 7 компании и конфиденциальные данные 8 по умолчанию не шифруются. Пользователь имеет возможность ввести пароль, когда желает использовать устройство 1 для конфиденциальных целей, что послужит причиной того, что данные, передающиеся удаленному хранилищу 12, будут шифроваться заранее, но только в установленный период времени. Со ссылкой на фиг.5, устройство 1 сконфигурировано для приема 70 ввода пароля. При вводе верного пароля устройство 1 просит пользователя выбрать период конфиденциальности, что может быть выбором из набора стандартных периодов, таких как, например, 30 минут, 6 часов и 1 неделя. Возможны и другие периоды времени, а пользователь может иметь возможность ввода любого времени вплоть до предварительно определенного максимума. Устройство 1 принимает 72 ввод требуемого промежутка времени конфиденциальности от пользователя и затем осуществляет мониторинг 74, истек или нет данный промежуток времени. Во время выбранного периода все данные 8 шифруются 76, используя секретный ключ 11, как в предположении, что все использование электронного устройства во время данного периода времени предназначено для конфиденциальных данных 8. Зашифрованные данные затем передаются 78 к удаленному хранилищу 12. Если 74 промежуток времени конфиденциальности истек 77, данные не шифруются, используя секретный ключ, как в предположении, что данные, созданные после этого периода времени являются данными 7 компании, которые передаются 78 к удаленному хранилищу 12 без шифрования (или шифруются, используя ключ 10 компании). После передачи 78 данных, зашифрованных или нет, процесс возвращается к началу на этап 74, чтобы время от времени могла выполняться проверка того, истек ли промежуток времени конфиденциальности, и могут ли быть переданы другие данные при необходимости.

Примерные правила

Следующее является примерами правил, которые могут использоваться для шифрования, используя секретный ключ пользователя:

1. Всегда шифруются. После кражи пользователь предоставляет ключ. Этот случай будет подходящим, если записываются данные о местоположении.

2. Всегда шифруются. Расшифровка данных возможна после того, как и пользователь, и владелец предоставят свои соответствующие части составного ключа.

3. Шифрование происходит согласно секретному ключу в периоды времени вне рабочего дня.

4. Как примерное правило (3), но это правило может быть модифицировано, чтобы учесть отпуска и варьируемое время работы.

5. Как примерное правило (3), но может быть активировано, только если пользователь введет пароль при перезагрузке или разблокировании.

6. Шифрование происходит согласно секретному ключу временно по запросу пользователя, как в варианте осуществления согласно фиг.5. Требуемый промежуток времени конфиденциальности может быть введен пользователем или может быть фиксирован. Это может быть различный период, зависящий от времени дня. Например, во время второго завтрака он может составлять 20 минут. Вечером он может составлять 5 часов. На выходных он может составлять целый день.

Альтернативы и вариации

Этапы на фигурах могут выполняться в порядке, отличном от того, который проиллюстрирован, или они могут быть объедены там, где показаны раздельно.

Сигнал (такой как слышимый сигнал или визуальное всплывающее сообщение, сформированное устройством) о том, что период секретного шифрования завершен, или близится к концу, может быть сформирован агентом и передан пользователю. Это может быть замаскированный сигнал, который не дает вору никакого понятия о том, что в устройстве установлена некая форма отслеживающей защиты.

Пароль пользователя для шифрования может быть удален агентом из устройства в конце каждого периода шифрования. Это предотвратит попытку вора использовать его для шифрования данных о местоположении, чтобы скрыть его местонахождение.

При предоставлении охранной компании секретного ключа пользователя система может быть сконфигурирована, чтобы только расшифровывать данные, отстоящие на конкретный период времени в прошлое, такой как две недели. Это может быть скомпоновано посредством регулярного удаления старых данных из удаленного устройства хранения. Альтернативно, секретный шифровальный ключ может использоваться как функция времени, так что данный ключ расшифровки может разблокировать только текущие и будущие данные, но не исторические данные.

Конфиденциальные данные и данные компании не обязательно передаются, как только они созданы. Они могут храниться локально в электронном устройстве 1 в их соответствующих хранилищах 7,8 данных, пока не будет доступно соединение между устройством 1 и центром 3 мониторинга, или пока не настанет время для агента инициировать связь или ответить центру 3 мониторинга.

В то время как вариант осуществления был описан в отношении к защите конфиденциальных данных о местоположении, раскрытый предмет изобретения может в равной степени применяться для защиты других конфиденциальных данных, созданных, используя совместно коммерчески и конфиденциально используемое устройство. Другие конфиденциальные данные, которые могут быть защищены, включают в себя данные использования, посещенные веб-сайты, проигрываемые видео- и аудиофайлы, загрузки, нажатия клавиш, моментальные снимки экранов, электронные письма, файлы и любые другие секретные данные.

Настоящее описание является описанием лучшего на данный момент продуманного метода осуществления предмета изобретения, раскрытого и заявленного в материалах настоящей заявки. Описание сделано с целью иллюстрации общих принципов предмета изобретения и не должно восприниматься в ограничительном смысле. Предмет изобретения может найти применение во множестве реализаций без отклонения от объема сделанного раскрытия, как будет очевидно специалистам в данной области из понимания принципов, которые лежат в основе предмета изобретения.

Формула изобретения

1. Способ, выполняемый пользовательским вычислительным устройством, для предоставления возможности мониторинга местоположения пользовательского вычислительного устройства из удаленного местоположения, при этом способ содержит этапы, на которых:

получают данные о местоположении, отражающие текущее местоположение пользовательского вычислительного устройства;

определяют на основании действия правила условного шифрования данных,

измененного или обновленного при осуществлении связи с удаленной системой мониторинга, шифровать ли данные о местоположении, используя секретный ключ пользователя пользовательского вычислительного устройства;

когда выполнено определение шифровать данные о местоположении, используя секретный ключ, шифруют данные о местоположении, используя секретный ключ, для формирования зашифрованных данных о местоположении и передают зашифрованные данные о местоположении по сети к системе мониторинга; и

когда выполнено определение не шифровать данные о местоположении, используя секретный ключ, передают данные о местоположении по сети к системе мониторинга без шифрования данных о местоположении секретным ключом,

при этом способ выполняется под управлением программного кода, исполняемого пользовательским вычислительным устройством.

2. Способ по п.1, дополнительно содержащий этап, на котором принимают передачу от удаленной системы мониторинга, которая инструктирует пользовательское вычислительное устройство прекращать шифрование, используя секретный ключ.

3. Способ по п.1, дополнительно содержащий этапы, на которых:

принимают аутентификацию от пользователя, и в результате упомянутой аутентификации, определяют шифровать данные о местоположении, используя секретный ключ, в течение предопределенного интервала.

4. Способ по п.3, в котором предопределенный интервал выбирается пользователем.

5. Способ по п.1, в котором определение основано, по меньшей мере частично, на времени суток, ассоциированном с данными о местоположении.

6. Способ по п.5, в котором определение основано дополнительно на дне недели, ассоциированном с данными о местоположении.

7. Способ по п.5, в котором определение основано дополнительно на дате, ассоциированной с данными о местоположении.

8. Способ по п.1, дополнительно содержащий этап, на котором передают данные приложений к упомянутой системе мониторинга для предоставления возможности вышеупомянутым данным приложений удаленно резервно копироваться, при этом упомянутые данные приложений являются отличными от упомянутых данных о местоположении.

9. Способ по п.8, дополнительно содержащий этап, на котором определяют на основании действия правила условного шифрования данных, шифровать ли данные приложений, используя секретный ключ, перед передачей к системе мониторинга.

10. Способ по п.9, в котором определение основано, по меньшей мере, частично на времени суток, ассоциированном с данными приложений.

11. Способ по п.10, в котором определение основано дополнительно на дне недели, ассоциированном с данными о местоположении.

12. Компьютерно-читаемый носитель, который хранит программный код, который инструктирует пользовательское вычислительное устройство выполнять способ, который содержит этапы получения данных о местоположении, отражающих текущее местоположение пользовательского вычислительного устройства;

определения на основании действия правила условного шифрования данных, измененного или обновленного во время связи с удаленной системой мониторинга, шифровать ли данные о местоположении, используя секретный ключ пользователя пользовательского вычислительного устройства;

когда выполнено определение шифровать данные о местоположении, используя

секретный ключ, шифрования данных о местоположении, используя секретный ключ, для формирования зашифрованных данных о местоположении, и передачи зашифрованных данных о местоположении по сети к системе мониторинга; и

когда выполнено определение не шифровать данные о местоположении, используя секретный ключ, передачи данных о местоположении по сети к системе мониторинга без шифрования данных о местоположении секретным ключом.

13. Система для зашиты конфиденциальных данных во время мониторинга электронного устройства, причем система содержит:

a. удаленную систему мониторинга;

b. электронное устройство, содержащее устройство обработки, память, в которой постоянно хранятся данные, и сетевой интерфейс;

c. модуль шифрования, инсталлированный в упомянутом электронном устройстве; и

d. правило условного шифрования, сохраненное в упомянутом устройстве;

при этом упомянутое устройство сконфигурировано для:

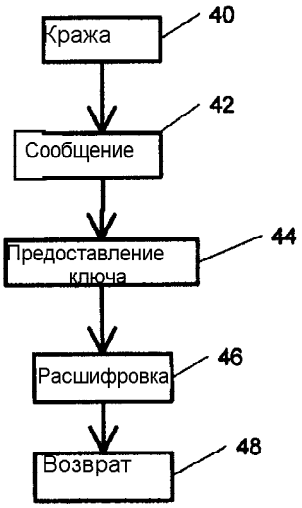
i. определения, что данные являются конфиденциальными данными или неконфиденциальными данными в соответствии с правилом, измененным или обновленным во время связи с удаленной системой мониторинга;

ii. шифрования конфиденциальных данных; и

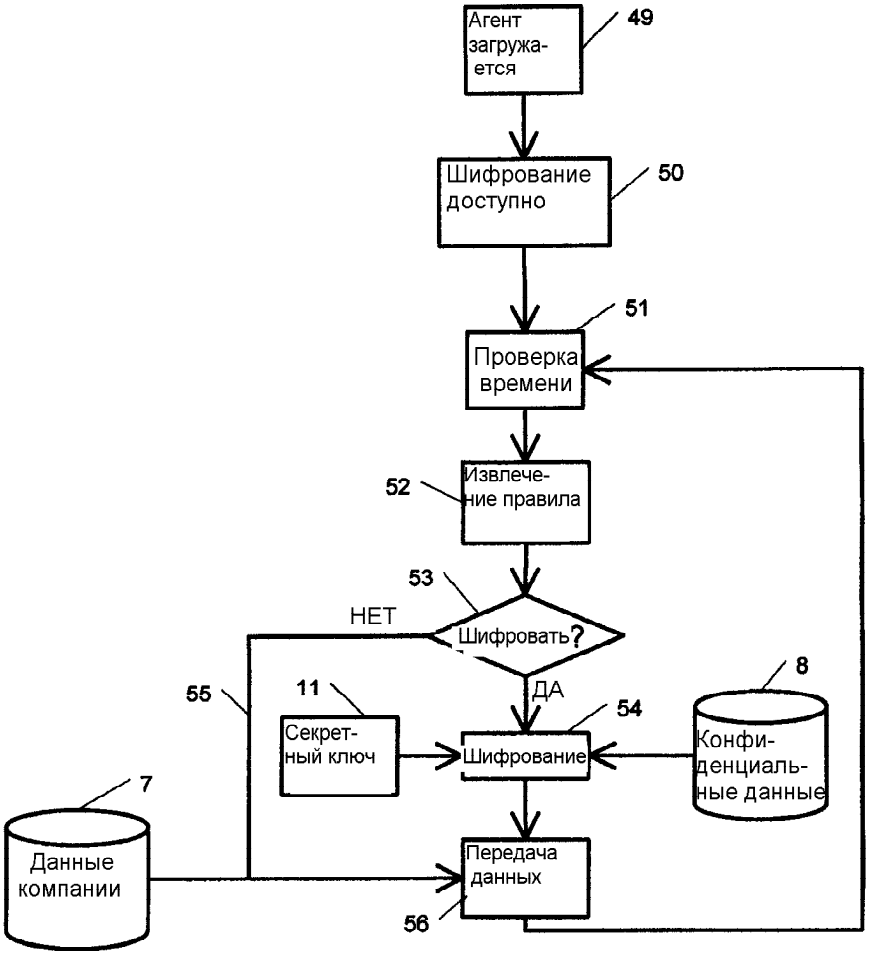
iii. передачи неконфиденциальных данных и зашифрованных конфиденциальных данных к удаленной системе мониторинга через сетевой интерфейс.

14. Система по п.13, в которой упомянутое устройство сконфигурировано для автоматического определения, являются ли данные конфиденциальными данными или неконфиденциальными данными, основываясь на расписании.

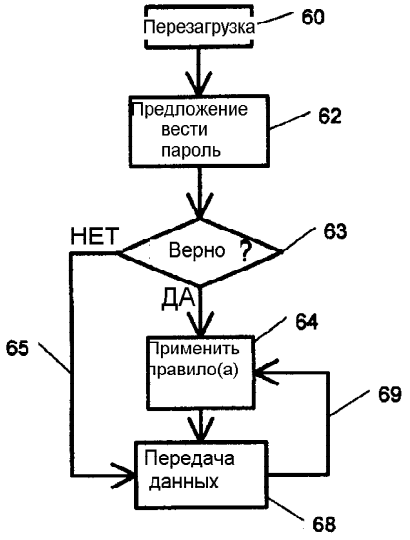
15. Система по п.13, в которой упомянутое устройство сконфигурировано для определения того, что данные являются конфиденциальными данными в течение некоторого периода времени и являются неконфиденциальными данными после упомянутого периода времени.


Кража
40
Сообщение
42
Предоставление ключа
44
Расшифровка
46
Возврат
48

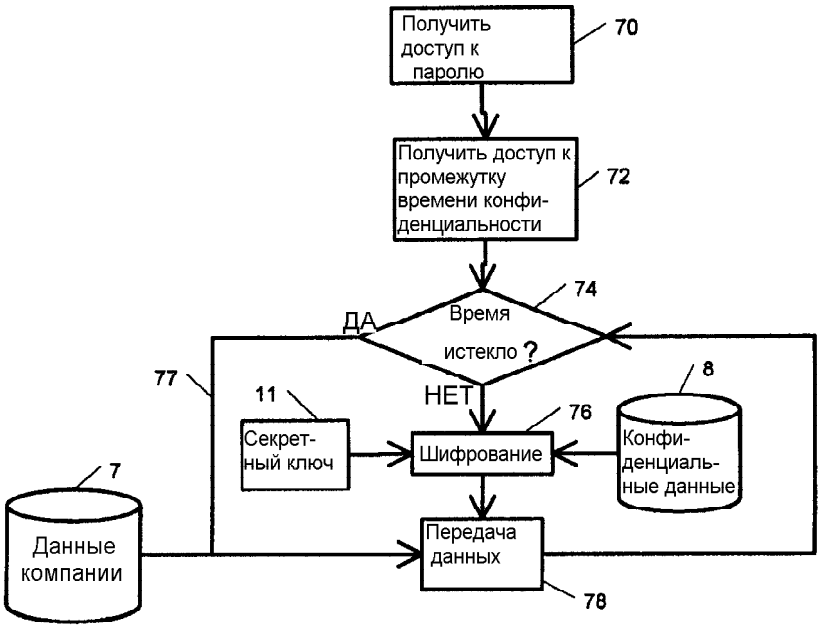
ФИГ.2


Агент загружа-ется
49
Шифрование доступно
50
Проверка времени
51
Извлече-ние правила
52
53
НЕТ
Шифровать?
ДА
55
11
Секрет-ный ключ
54
Шифрование
8
Конфи-денциаль-ные данные
7
Данные компании
Передача данных
56

ФИГ.3


Перезагрузка
60
Предложение вести пароль
62
НЕТ
Верно ?
63
ДА
64
65
Применить правило(а)
69
Передача данных
68

ФИГ.4


Получить доступ к паролю
70
Получить доступ к промежутку времени конфиденциальности
72
74
ДА
Время истекло ?
НЕТ
77
11
Секретный ключ
76
Шифрование
8
Конфиденциальные данные
7
Данные компании
Передача данных
78

ФИГ.5