РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 665 247**(13) **C1**

(51) МПК
G06F 15/173 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
G06F 15/00 (2006.01)

(21)(22) Заявка: **2017137602, 27.10.2017**

(24) Дата начала отсчета срока действия патента:
27.10.2017

Дата регистрации:
28.08.2018

Приоритет(ы):
(22) Дата подачи заявки: **27.10.2017**

(45) Опубликовано: **28.08.2018** Бюл. № **25**

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):
Ерыгин Александр Витальевич (RU)

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

(56) Список документов, цитированных в отчете о поиске: **US 2005/0278534 A1, 15.12.2005. RU 2571381 C1, 20.12.2015. US 20030237004 A1, 25.12.2003. US 20040030888 A1, 12.02.2004. US 2005/0228998 A1, 13.10.2005.**

(54) Способ доставки сертификатов в защищенной сетевой вычислительной системе

(57) Реферат:

Изобретение относится к технологиям сетевой связи. Технический результат заключается в повышении безопасности передачи данных. Способ доставки сертификатов в защищенной сетевой вычислительной системе, которая содержит сервер распространения, причем сервер включает установленное на нем средство распространения, выполненное с возможностью: хранить сертификаты; принимать запросы от компьютеров пользователей на загрузку сертификатов; передавать сертификаты в ответ на запросы от компьютеров пользователей; а также компьютеры пользователей, причем каждый компьютер включает средство установки сертификатов, выполненное с возможностью перехватывать запросы на загрузку сертификатов от компьютера пользователей к внешним по отношению к вычислительной системе удостоверяющим центрам; перенаправлять запросы на загрузку сертификатов от компьютера пользователя к средству распространения; принимать сертификаты; устанавливать сертификаты на компьютер пользователя.

RU 2665247 C1

RU 2665247 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 665 247**(13) **C1**

(51) Int. Cl.
G06F 15/173 (2006.01)

(12) ABSTRACT OF INVENTION

(52) CPC
G06F 15/00 (2006.01)

(21)(22) Application: **2017137602, 27.10.2017**

(24) Effective date for property rights:
27.10.2017

Registration date:
28.08.2018

Priority:
(22) Date of filing: **27.10.2017**

(45) Date of publication: **28.08.2018** Bull. № **25**

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

(72) Inventor(s):
Erygin Aleksandr Vitalevich (RU)

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

RU 2665247 C1

(54) METHOD OF DELIVERING CERTIFICATES IN PROTECTED NETWORK COMPUTING SYSTEM

(57) Abstract:

FIELD: network communication technologies.

SUBSTANCE: invention relates to the network communication technologies. Method for delivering certificates in a secure networked computing system that includes a distribution server, the server including a distribution medium installed thereon configured to: store certificates; receive requests from users' computers to download certificates; send certificates in response to requests from users' computers; as well as users' computers, each computer including a certificate installer configured to intercept requests for the download of certificates from the user's computer to the authentication centers external to the computing system; redirect requests to download certificates from the user's computer to the distribution tool; accept certificates; install certificates on the user's computer.

EFFECT: technical result is improved data transmission security.

1 cl

RU 2665247 C1

Область техники, к которой относится изобретение

Изобретение относится к вычислительной технике, инфраструктуре открытых ключей и способам обновления списков аннулированных сертификатов и может быть использовано для доставки списков аннулированных сертификатов на компьютер пользователя.

Уровень техники

В настоящее время в сетевых вычислительных системах широко используются технологии на основе инфраструктуры открытых ключей (public key infrastructure, далее - PKI). Неотъемлемой частью PKI являются сертификаты, сформированные в электронном виде с использованием криптографического стандарта X509. Такой сертификат подписывается закрытым ключом удостоверяющего центра (УЦ). Имея сертификат с открытым ключом, для УЦ не составляет труда убедиться, что проверяемый сертификат выпущен доверенным УЦ. В случае если секретный ключ был скомпрометирован, УЦ отзывает сертификат открытого ключа. После отзыва сертификата он считается недействительным. Использование недействительного сертификата несет угрозу информационной безопасности, поэтому сведения об отзыве сертификатов должны быть как можно более оперативно доставлены и установлены на персональные компьютеры (ПК) пользователей.

В настоящее время используются следующие способы проверки действительности сертификата:

1) на основе списка аннулированных сертификатов (CAC), выпускаемых УЦ с некоторой периодичностью, при этом актуальный CAC должен быть предварительно получен и использован системой, осуществляющей проверку сертификата;

2) на основе запроса к УЦ по протоколу OCSP (Online Certificate Status Protocol, https://tools.ietf.org/html/rfc4806) и последующего получения информации о статусе сертификата.

Известен способ пополнения базы данных доверенных сертификатов, использующейся при антивирусной проверке (патент РФ №2571381, приоритет от 17.10.2014 г.), в котором получают идентификатор конечного сертификата открытого ключа цифровой подписи файла, отсутствующий в базе данных доверенных сертификатов; получают файл; определяют содержащийся в полученном файле конечный сертификат открытого ключа цифровой подписи упомянутого файла; проверяют действительность конечных сертификатов; задают уровень доверия для конечных сертификатов; пополняют базу данных сертификатами и определенными уровнями доверия сертификатов.

Недостатком известного способа является невысокий уровень надежности проверки сертификата, если он получен от нескольких пользователей сети, а также необходимость запроса к УЦ, внешнего по отношению к внутренней сети.

Известен также способ проверки действительности цифровых сертификатов вычислительными объектами в системе обработки данных (патент США №7444509, приоритет от 27.05.2004 г.), в котором проверка действительности сертификатов осуществляется путем запроса к сетевой службе состояния CAC и УЦ, причем в ходе проверки также может устанавливаться и проверяться вся цепочка сертификатов, вплоть до конечного.

Недостатком данного способа является двукратный запрос к УЦ, внешним по отношению к внутренней сети, что увеличивает сложность реализации, а также необходимость запроса к УЦ, внешнего по отношению к внутренней сети.

Этот способ принимается в качестве прототипа.

Известные способы, к сожалению, не подходят для случая, когда защищенная сетевая вычислительная система должны работать в закрытом контуре, внутри которого

отсутствует доступ к внешним по отношению к системе УЦ и узлам, обеспечивающим сервис OCSP.

Прикладные программы, при использовании сертификата стандарта X509, должны осуществить проверку действительности сертификата. При этом обычно проверяются срок действия открытого ключа, срок действия закрытого ключа, параметры использования ключа, факт отзыва сертификата.

Адрес узла, по которому необходимо запросить сведения о сертификате (или несколько адресов разных узлов), относится, как правило, к глобальной сети Интернет, записан в сертификате и не подлежит изменению. Прикладная программа при проверке сертификата должна оперировать именно данным адресом.

Если адрес узла, по которому необходимо запросить сведения о сертификате, находится вне закрытого контура защищенной сети, то запрос становится невозможен, проверка сертификата не может быть осуществлена и возникает угроза информационной безопасности.

В таком случае системный администратор вынужден заранее получить сертификаты и/или CAC за пределами закрытого контура, а затем последовательно вручную распространять полученные CAC на ПК пользователей, что весьма трудоемко и затратно.

Раскрытие изобретения

Техническим результатом является:

1) обеспечение доставки сертификатов на ПК пользователей, находящихся в закрытом контуре и не имеющих доступа к внешним УЦ;

2) обеспечение автоматизации процесса установки сертификатов на ПК пользователей.

Для этого предлагается способ доставки сертификатов в защищенной сетевой вычислительной системе, которая содержит

• сервер распространения, причем сервер включает установленное на нем средство распространения, выполненное с возможностью

- хранить сертификаты,
- принимать запросы от компьютеров пользователей на загрузку сертификатов,
- передавать сертификаты в ответ на запросы от компьютеров пользователей;

• компьютеры пользователей, причем каждый компьютер включает средство установки сертификатов, выполненное с возможностью

- перехватывать запросы на загрузку сертификатов от компьютера пользователей к внешним по отношению к вычислительной системе удостоверяющим центрам,
- перенаправлять запросы на загрузку сертификатов от компьютера пользователя к средству распространения;
- принимать сертификаты;
- устанавливать сертификаты на компьютер пользователя;

способ, заключающийся в том, что

• доставляют сертификаты в сервер распространения доверенным способом;

• вносят сведения о сервере распространения в средство установки каждого компьютера пользователя;

• перехватывают на каждом компьютере с помощью средства установки все запросы к внешним по отношению к вычислительной системе удостоверяющим центрам на загрузку сертификатов;

• перенаправляют все перехваченные запросы к серверу распространения;

• передают сертификаты в ответ на запросы с помощью средства распространения в компьютеры пользователей;

• принимают на компьютере пользователя с помощью средства установки сертификаты, полученные из средства распространения;

• устанавливают сертификаты на компьютере пользователя с помощью средства установки.

Необходимо отметить, что предлагаемый способ может быть использован как для доставки действующих сертификатов, так и CAC.

Для реализации предлагаемого способа предварительно необходимо сформировать средство распространения и средство установки сертификатов, способные выполнять указанные выше функции, причем, в зависимости от различных конкретных факторов, эти средства могут быть программно-аппаратными или программными. После изготовления средство распространения устанавливается на выбранный в вычислительной системе сервер распространения, а средство установки сертификатов устанавливается на каждый компьютер пользователя в вычислительной системе.

Затем необходимо определить, какие сертификаты необходимы в вычислительной системе (действующие и/или CAC), получить сертификаты из соответствующих УЦ и доверенным способом доставить сертификаты в сервер распространения.

Для этого системный администратор защищенной сетевой вычислительной системы проводит контроль программного обеспечения (ПО), установленного на ПК пользователей, и выявляет ПО, для работы которого необходима инфраструктура PKI. Для каждого такого ПО администратор выясняет список необходимых сертификатов УЦ, адреса точки распространения сертификатов для данных УЦ, которые обычно находятся в открытом доступе. Далее администратор за пределами защищенного контура получает сертификаты УЦ и/или CAC, сохраняет их на носитель и доставляет в закрытый контур.

Затем системный администратор в закрытом контуре копирует файлы с носителя в выделенную папку на сервере распространения, предварительно авторизовавшись на нем. После копирования на сервер распространения администратор заполняет список узлов в защищенной сети, с которыми средство распространения будет работать, устанавливать и обновлять сертификаты УЦ или CAC. Сертификаты УЦ и CAC имеют ограниченный срок действия. Администратор должен осуществлять доставку сертификатов УЦ и CAC в закрытый контур до истечения срока действия установленных сертификатов УЦ или CAC на ПК пользователей.

Непосредственно перед реализацией предложенного способа необходимо определить параметры передачи данных между средством распространения и средством установки (протокол передачи данных, скорость передачи данных), параметры безопасности (защиты канала передачи данных, аутентификации и идентификации).

Затем пользователи могут непосредственно приступить к работе в защищенной сетевой вычислительной системе.

Если в процессе работы средства защиты информации на компьютерах пользователей высылают запросы к внешним по отношению к вычислительной системе удостоверяющим центрам на загрузку сертификатов, то на каждом компьютере с помощью средства установки все запросы к внешним по отношению к вычислительной системе удостоверяющим центрам на загрузку сертификатов перехватываются и перенаправляются к серверу распространения.

В ходе процесса перехвата в средстве установки проводится контроль адресов сетевых

запросов и определение адресов, относящихся к внешним ресурсам, после чего адреса в запросах заменяются на адрес сервера распространения, и запросы отправляются по сети.

В ответ на запросы с помощью средства распространения сертификаты передаются в компьютеры пользователей, после чего сертификаты устанавливаются на компьютере пользователя с помощью средств установки.

В результате, средства защиты информации на компьютерах пользователей смогут автоматически проверять используемые сертификаты.

Предложенный способ позволяет автоматически доставить и установить CAC на ПК пользователей, работающих в закрытом контуре, сократить трудозатраты системного администратора на установку CAC на ПК пользователей, повышает безопасность систем, использующих PKI, путем снижения количества ошибок проверки сертификатов за счет ускорения процесса доставки и установки CAC на ПК пользователей.

Осуществление изобретения

Для реализации предложенного способа в защищенной сетевой вычислительной системе необходимо сначала выделить какой-либо компьютер, который будет служить в качестве сервера распространения. Предпочтительно, это должен быть отдельный компьютер, подключенный к сети, с достаточными аппаратными ресурсами и установленным общесистемным и серверным ПО, например, это может быть компьютер на базе процессора Intel, имеющим тактовую частоту 3,5 ГГц, с оперативной памятью 16 Гбайт, с операционной системой Debian 8 и жестким диском объемом 2 Тбайт.

Для реализации предлагаемого способа предварительно необходимо сформировать средство распространения и средство установки сертификатов, способное выполнять указанные выше функции, причем, в зависимости от различных конкретных факторов, предпочтительно, эти средства выполняются в виде прикладных программ.

Сформировать программы, выполняющие функции средства распространения и средства установки сертификатов, может специалист в области программирования (программист).

После формирования и тестирования средство распространения устанавливается на сервер распространения, а средство установки сертификатов устанавливается на каждый компьютер пользователя в вычислительной системе.

Затем системный администратор определяет конкретный сетевой адрес, по которому будут поступать запросы в средство распространения на сервере распространения (из имеющегося в распоряжении списка доступных адресов в вычислительной системе), а также порт и протокол доступа (например, протокол TCP/IP). Непосредственно перед реализацией предложенного способа необходимо определить параметры передачи данных между средством распространения и средством установки (протокол передачи данных, скорость передачи данных), параметры безопасности (защиты канала передачи данных, аутентификации и идентификации).

После этого системный администратор проводит контроль ПО, установленного на ПК пользователей, и выявляет ПО, для работы которого необходима инфраструктура PKI. Для каждого такого ПО администратор выясняет список необходимых сертификатов УЦ, адреса точки распространения сертификатов для данных УЦ, которые обычно находятся в открытом доступе. Далее администратор за пределами защищенного контура получает сертификаты УЦ и/или CAC, сохраняет их на носителе и доставляет в закрытый контур.

Затем системный администратор в закрытом контуре копирует файлы с носителя в

выделенную папку на сервере распространения. После копирования на сервер распространения администратор заполняет список узлов в защищенной сети, с которыми средство распространения будет работать, устанавливать и обновлять сертификаты УЦ или САС.

Для хранения сертификатов УЦ и САС может быть использована какая-либо система управления базами данных, например PostgreSQL, или аналогичная.

После выполнения указанных выше предварительных действий предложенный способ может быть непосредственно выполнен.

Пользователи сети работают на своих ПК в сети в обычном режиме.

В случае, если в процессе работы средства защиты информации на ПК пользователей высылают запросы к внешним по отношению к вычислительной системе УЦ на загрузку сертификатов, то на ПК с помощью средства установки все запросы к внешним по отношению к вычислительной системе УЦ на загрузку сертификатов перехватываются и перенаправляются к серверу распространения.

В ходе процесса перехвата в средстве установки проводится контроль адресов сетевых запросов и определение адресов, относящихся к внешним ресурсам, после чего адреса в запросах заменяются на адрес сервера распространения, и запросы отправляются по сети.

В ответ на запросы с помощью средства распространения сертификаты передаются в компьютеры пользователей, после чего сертификаты устанавливаются на компьютере пользователя с помощью средств установки.

Соответственно средства защиты информации на компьютерах пользователей смогут автоматически проверять используемые сертификаты.

В результате обеспечивается доставка сертификатов на ПК пользователей, находящихся в закрытом контуре и не имеющих доступа к внешним УЦ, и обеспечивается автоматизация процесса установки сертификатов на ПК пользователей.

Для пользователей процедуры проверки и установки сертификатов проходят незаметно, поскольку все действия способа выполняются автоматически.

(57) Формула изобретения

Способ доставки сертификатов в защищенной сетевой вычислительной системе, которая содержит: сервер распространения, причем сервер включает установленное на нем средство распространения, выполненное с возможностью хранить сертификаты, принимать запросы от компьютеров пользователей на загрузку сертификатов, передавать сертификаты в ответ на запросы от компьютеров пользователей; компьютеры пользователей, причем каждый компьютер включает средство установки сертификатов, выполненное с возможностью перехватывать запросы на загрузку сертификатов от компьютера пользователей к внешним по отношению к вычислительной системе удостоверяющим центрам, перенаправлять запросы на загрузку сертификатов от компьютера пользователя к средству распространения, принимать сертификаты, устанавливать сертификаты на компьютер пользователя, заключающийся в том, что доставляют сертификаты в сервер распространения доверенным способом, вносят сведения о сервере распространения в средство установки каждого компьютера пользователя, перехватывают на каждом компьютере с помощью средства установки все запросы к внешним по отношению к вычислительной системе удостоверяющим центрам на загрузку сертификатов, перенаправляют все перехваченные запросы к серверу распространения, передают сертификаты в ответ на запросы с помощью средства распространения в компьютеры пользователей, принимают на компьютере

пользователя с помощью средства установки сертификаты, полученные из средства распространения, устанавливают сертификаты на компьютере пользователя с помощью средства установки.