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

Усиленная аутентификация в операционной системе

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 631 группы
специальности 090102.65 «Компьютерная безопасность»
факультета компьютерных наук и информационных технологий
Грачева Павла Алексеевича

Научный руководитель
ассистент Н.Н. Бондарев

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

Саратов 2016

ВВЕДЕНИЕ

Безопасность информации является стратегической целью постиндустриального общества. Безопасными должны быть все процессы производства, хранения и обмена информацией, все технические и программные компоненты, участвующие в этих процессах.

Основными задачами информационной безопасности являются:

- обеспечение конфиденциальности информации;
- обеспечение целостности и достоверности информации;
- обеспечение юридической значимости информации;
- обеспечение доступности информации и информационных ресурсов.

Градация приоритетов среди перечисленных задач информационной безопасности является вопросом, решаемым только в конкретных условиях применения, и зависит от требований, предъявляемых непосредственно к информационным системам.

В современных информационных системах хранится огромное количество информации. Часть ее общедоступна, и с нею может ознакомиться любой желающий. Однако кроме общедоступной информации в базах данных может храниться служебная, коммерческая или государственная тайна, персональные данные или просто личная информация пользователя. Для этой информации необходимо выполнение свойства конфиденциальности. Но если закрытая информация (информация ограниченного доступа) имеется, значит, она должна быть доступна только тем субъектам (пользователям), кому она доверена. Права доступа субъектов к объектам (информации) регламентируются совокупностью правил, которые называются правилами разграничения доступа.

Существуют разные способы обработки информации – например, один пользователь может работать со всей информацией только в режиме чтения, а другому разрешается читать и изменять объекты доступа, а также уничтожать их и создавать новые. Таким образом, концепция разграничения доступа предусматривает следующее условие: прежде чем допустить кого-либо к информации, необходимо определить полномочия этого пользователя, а для этого

нужно сначала его идентифицировать. Для идентификации ему выдается некоторый идентификатор, который должен быть предъявлен для доступа к информации. А проверка принадлежности пользователю предъявленного им идентификатора называется аутентификацией.

Существует большое количество способов аутентификации, среди которых наиболее распространенной до сих пор остается парольная защита. Однако из-за ее серьезных недостатков в последнее время все большую актуальность приобретает так называемая усиленная аутентификация – процедура проверки, при которой используются более надежные методы.

Усиленная аутентификация внедряется в настоящее время повсеместно. Такая защита применяется, например, в почтовых сервисах, сервисах электронных платежей, в социальных сетях, на порталах государственных услуг для защиты учетных записей пользователей, а также в операционных системах для разграничения доступа к информации, хранящейся на компьютере.

Цель дипломной работы – рассмотреть принципы работы и использования различных средств аутентификации, а также реализовать усиленную аутентификацию в операционной системе Windows с использованием съемных носителей информации.

Для достижения цели необходимо выполнить следующие задачи:

1) рассмотреть и проанализировать существующие варианты усиленной аутентификации;

2) разработать поставщик учетных данных (Credential Provider) для защиты входа в систему Windows;

3) разработать службу Windows для контроля подключенного носителя информации при работе с Windows;

4) разработать приложение для администрирования средства двухфакторной аутентификации.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Дипломная работа состоит из введения, двух разделов (трех подразделов), заключения, списка использованных источников и трех приложений.

В первом разделе «Усиленная аутентификация как способ защиты информации» анализируются базовые понятия, позволяющие раскрыть основное содержание усиленной аутентификации. В первом подразделе «Аутентификация пользователей. Факторы аутентификации» вводятся понятия аутентификации и ее факторов, перечисляются основные их виды.

Подсистема аутентификации пользователей – важнейший компонент корпоративной системы информационной безопасности, и ее значение трудно переоценить. Подсистема аутентификации подтверждает личность пользователя информационной системы и поэтому должна быть надежной и адекватной, то есть исключать все ошибки в предоставлении доступа. Существующие методы аутентификации различны по степени надежности, и, как правило, с усилением защиты резко возрастает цена систем, что требует при выборе средств аутентификации анализа рисков и оценки экономической целесообразности применения тех или иных мер защиты. Однако в последнее время «соотношение сил» в области эффективности применяемых методов аутентификации меняется.

Средства аутентификации можно разделить на три группы («фактора») в соответствии с применяемыми принципами: принцип «что Вы знаете» («you know»), лежащий в основе методов аутентификации по паролю; принцип «что Вы имеете» («you have»), когда аутентификация осуществляется с помощью магнитных карт, токенов и других устройств; и принцип «кто Вы есть» («you are»), использующий персональные свойства пользователя (отпечаток пальца, структуру сетчатки глаза и т.д.).

Каждый фактор аутентификации обладает собственными отличительными характеристиками и недостатками.

Основными факторами аутентификации являются пароль, устройство аутентификации и биометрика. Каждый из факторов обладает недостатками, и не существует одного самого лучшего способа аутентификации. Выбор зависит от рисков, с которыми может столкнуться информационная система, и от затрат. Однако не всегда отдельно взятый фактор может обеспечить требуемый уровень защиты. В таких случаях применяется усиленная аутентификация.

Во втором подразделе «Понятие усиленной аутентификации» дается определение усиленной аутентификации, указываются ее разновидности и способы реализации.

Усиленная аутентификация основывается не только на применении более совершенных и надежных технологий, но и на использовании нескольких факторов аутентификации при проверке пользователей. Такие системы называются системами многофакторной аутентификации.

Системы двухфакторной аутентификации являются наиболее распространенными и используют два разных фактора при аутентификации пользователей. Она используется в основном в сетевых сервисах, однако и для операционных систем является не менее актуальной.

Очевидно, что двухфакторная аутентификация представляет собой одну из следующих комбинаций аутентификационных факторов: пароль + устройство, пароль + биометрика, устройство + биометрика.

Для реализации усиленной аутентификации (в т.ч. и многофакторной аутентификации) удобнее всего использовать средства трех групп:

- аппаратно-программные модули доверенной загрузки (АПМДЗ);
- программные комплексы под общим названием «средства защиты от НСД»;
- программные комплексы, рассчитанные лишь на реализацию двухфакторной аутентификации.

Однако важно не количество факторов и не типы предъявляемых признаков, а качество реализации механизма на обеих сторонах взаимодействия – как в пользовательской части, так и в части, находящейся у проверяющей стороны.

В третьем подразделе «Существующие решения для двухфакторной аутентификации» рассматривается несколько наиболее крупных производителей средств усиленной аутентификации.

Разнообразие продукции в области аутентификации пользователей позволяет потребителям найти необходимые средства усиленной аутентификации в соответствии с предпочтениями и стоимостью.

Во втором разделе «Реализация двухфакторной аутентификации с использованием съемных носителей информации» описывается средство двухфакторной аутентификации, разработанное в процессе выполнения дипломной работы.

В качестве основы была выбрана парольная аутентификация в операционной системе Windows, однако она была усилена с помощью механизма проверки принадлежности пользователю предъявляемого системе USB-носителя информации.

Возможности реализованного средства аутентификации:

1) двухфакторная аутентификация на основе USB-носителей;
2) аварийный вход администратора в систему;
3) блокировка рабочей станции при извлечении носителя;
4) ограничение времени работы пользователей;
5) регистрация вносимых изменений в журнал;
6) отправка электронных сообщений на почту администратора в случае попыток несанкционированного доступа;
7) изменение политик безопасности: паролей, аудита и блокировки учетных записей;
8) хранение настроек программы в зашифрованном виде.

Разработанное средство аутентификации состоит из трех компонентов:

1) поставщик учетных данных (Credential Provider) для ОС Windows;
2) служба ОС Windows для контроля носителя;
3) программа администрирования установленной защиты.

Основным элементом является поставщик учетных данных, использующий комбинированный подход. Другими словами, для доступа к системе необходимо ввести пароль, предъявить зарегистрированный USB-носитель и ввести PIN-код, соответствующий данному носителю.

Администратор имеет возможность зайти в систему и без зарегистрированного для него носителя информации. Данный способ необходим в случае возникших проблем с устройством администратора.

Воспользоваться аварийным входом может только администратор, попытка такого входа обычным пользователем запрещена (при этом он увидит сообщение о запрете входа) и приравнивается к попытке несанкционированного доступа.

В случае попыток входа без носителя или с неверными данными, а также при попытке несанкционированного аварийного входа в систему на электронную почту администратора отправляются сообщения с краткой информацией об инциденте. Если отправка сообщений невозможна по причине отсутствия подключения к интернету, вся информация о попытках входа накапливается и отправляется при появлении такой возможности.

Также элементом реализованной защиты является служба Windows, которая отслеживает отключение носителей от компьютера.

Служба запускается от имени Local System и стартует автоматически до загрузки процесса winlogon.exe, т.е. до входа пользователя в систему. Основной задачей службы является перехват событий операционной системы об отключении устройств и блокировка системы в том случае, если отключен носитель текущего пользователя.

Еще одной функцией данной службы является отправка сообщений о попытках несанкционированного доступа администратору в том случае, если это по какой-либо причине не сделал поставщик учетных данных.

Третьим компонентом защиты является приложение для установки, администрирования и удаления защиты. Данное приложение позволяет регистрировать носители для пользователей, ограничивать время их работы, а также управлять политиками безопасности. В частности, можно изменять политики паролей (журнал паролей, сроки их действия, сложность и т.д.), политики блокировки учетных записей (количество ошибок ввода, время до сброса счетчика ошибок и продолжительность) и политики аудита различных событий.

Дополнительно предусмотрены настройки уведомлений администратора о попытках несанкционированного доступа в систему. Администратору предлагается ввести адрес электронной почты, на которую будут поступать уведомления, а также информацию о почтовом сервере (адреса отправителя и почтового сервера, пароль).

Для возможности контроля изменений настроек (таких как регистрация и удаление носителей пользователей, изменение времени входа, политик безопасности, информации о почтовом сервере и т.д.) они записываются в файл в директории программы.

Вся аутентификационная информация хранится в реестре в зашифрованном виде. Для этого используется алгоритм симметричного шифрования AES. Все настройки политик безопасности расположены в защищенных от доступа разделах реестра.

Следует отметить, что вносить изменения в реестр и устанавливать службы может только администратор системы, следовательно, данное приложение необходимо запускать от имени администратора.

В приложении А «Реализация Credential Provider» представлен фрагмент кода поставщика учетных данных для операционной системы Windows, в

приложении Б «Реализация службы для контроля носителя» – код службы, являющейся компонентом разработанного средства, а в приложении В «Реализация приложения для управления защитой» – фрагмент кода программы для администрирования защиты.

ЗАКЛЮЧЕНИЕ

В рамках данной дипломной работы были рассмотрены различные способы аутентификации и некоторые существующие программные решения. В результате проделанной работы реализовано средство усиленной аутентификации в операционной системе Windows с использованием съемных носителей информации.

Разработанное средство позволяет усилить аутентификационные процессы и, значит, повысить безопасность системы. Достигается это за счет использования съемных носителей информации в качестве дополнительного фактора аутентификации. Кроме того, вся информация о пользователях системы хранится в реестре в зашифрованном виде.

Согласно поставленным задачам разработанное средство состоит из трех компонентов: поставщика учетных данных (Credential Provider) для защиты входа в систему Windows, службы Windows для контроля подключенного носителя информации, приложения для администрирования средства двухфакторной аутентификации.

В разработанном средстве аутентификации реализованы следующие возможности: аварийный вход администратора в систему, блокировка рабочей станции при извлечении носителя, ограничение времени работы пользователей, регистрация вносимых изменений в журнал, отправка электронных сообщений на почту администратора в случае попыток несанкционированного доступа, изменение политик безопасности (паролей, аудита и блокировки учетных записей). Кроме того, администратор может настроить данное средство в соответствии с требованиями безопасности.

Основным преимуществом данного средства является то, что пользователи могут использовать любые USB-носители информации, при этом аутентификационные данные не записываются на носители, что позволяет использовать их по прямому назначению.

Таким образом, цель, состоящая в рассмотрении принципов работы и использования различных средств аутентификации, а также реализации усиленной аутентификации в операционной системе Windows с использованием съемных носителей информации, была достигнута и все задачи были выполнены.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1) Аутентификация пользователей – современные методы [Электронный ресурс] / TopS BI [Электронный ресурс]. – URL: http://topsbi.ru/default.asp?artID=848 (дата обращения: 05.10.2015). Загл. с экрана. Яз.рус.

2) Гриффин Дэн. Настройка входа в систему с помощью Credential Provider в Windows Vista [Электронный ресурс] / Дэн Гриффин // MSDN Magazine. Русская редакция. М.: Издательство «Русская редакция», 2002. №2 – URL: http://files.ligarobotov.ru/download.php?filename=files/library/%C6%F3%F0%ED%E0%EB%FB/MSDN 2002 - 2007/ 2007/02_February/MSDN_Mag_RE_2007_02.pdf (дата обращения: 08.10.2015). Загл. с экрана. Яз.рус.

3) Доля Алексей. Обзор рынка средств многофакторной аутентификации [Электронный ресурс] / КомпьютерПресс [Электронный ресурс]. – URL: http://compress.ru/article.aspx?id=15848 (дата обращения: 03.12.2015). Загл. с экрана. Яз.рус.

4) Идентификация и аутентификация [Электронный ресурс] / Refleader [Электронный ресурс]. – URL: http://refleader.ru/jgemerrnaotr.html (дата обращения: 05.12.2015). Загл. с экрана. Яз.рус.

5) Изменение параметров политики паролей [Электронный ресурс] / Windows [Электронный ресурс]. – URL: http://windows.microsoft.com/ru-ru/windows/change-password-policy-settings#1TC=windows-7 (дата обращения: 06.12.2015). Загл. с экрана. Яз.рус. Код безопасности [Электронный ресурс]. – URL: http://www.securitycode.ru (дата обращения: 06.12.2015). Загл. с экрана. Яз.рус.

6) Код безопасности [Электронный ресурс]. – URL: http://www.securitycode.ru (дата обращения: 06.12.2015). Загл. с экрана. Яз.рус.

7) Музыкантский А.И., Фурин В.В. Лекции по криптографии. – М.: МЦНМО, 2010. – С. 28-29.

8) Недостатки популярных методов аутентификации [Электронный ресурс] / Доверие в Сети [Электронный ресурс]. – URL: http://довериевсети.рф/article/57 (дата обращения: 06.10.2015). Загл. с экрана. Яз.рус.

9) Особенности применения двухфакторной аутентификации [Электронный ресурс] / InformationSecurity [Электронный ресурс]. – URL: http://www.itsec.ru/articles2/concept/osob_primenen_dvuhfakt_autentifik (дата обращения: 06.10.2015). Загл. с экрана. Яз.рус.

10) Парканти Шарат, Болле Рууд М., Джейн Энил. Биометрия: будущее идентификации [Электронный ресурс] / Открытые системы [Электронный ресурс]. – URL: http://www.osp.ru/os/2000/03/177933 (дата обращения: 06.12.2015). Загл. с экрана. Яз.рус.

11) Парольная аутентификация [Электронный ресурс] / Методы и средства защиты компьютерной информации [Электронный ресурс]. – URL: http://www.volpi.ru/umkd/zki/index.php?man=1&page=23 (дата обращения: 04.12.2015). Загл. с экрана. Яз.рус.

12) Продукты BioLink [Электронный ресурс] / BioLink. Биометрические системы [Электронный ресурс]. – URL: http://www.biolink.ru/products (дата обращения: 06.12.2015). Загл. с экрана. Яз.рус.

13) Смарт-карта [Электронный ресурс] / Энциклопедия экономиста! [Электронный ресурс]. – URL: http:// www.grandars.ru/student/bankovskoe-delo/smart-karta.html (дата обращения: 05.12.2015). Загл. с экрана. Яз.рус.

14) Смит Р.Э. Аутентификация: от паролей до закрытых ключей [Электронный ресурс] / Смит Р.Э. – М.: Издательский дом «Вильямс», 2002. – URL: http://computersbooks.net/index.php?id1=4&category=rukovodstvo-po-po&author=smit-re&book=2002&page=23 (дата обращения: 05.10.2015). Загл. с экрана. Яз.рус.

15) Токены vs Пароли [Электронный ресурс] / Хабрахабр [Электронный ресурс]. – URL: http://habrahabr.ru/post/ 126828 (дата обращения: 04.12.2015). Загл. с экрана. Яз.рус.

16) Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 31.12.2014) "Об информации, информационных технологиях и о защите информации" [Электронный ресурс] : (с изм. и доп., вступ. в силу с 01.09.2015). Доступ из справочно-правовой системы «Консультант». – URL: http://www.consultant.ru/ document/cons_doc_LAW_61798/0e9ec16b786dcbdaaa7f44abfc4a15e601d5be22 (дата обращения: 02.12.2015). Загл. с экрана. Яз.рус.

17) Шаров Владислав. Биометрические методы компьютерной безопасности [Электронный ресурс] / BYTE Россия [Электронный ресурс]. – URL: http://www.bytemag.ru/articles/detail.php?ID=6719 (дата обращения: 06.12.2015). Загл. с экрана. Яз.рус.

18) Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие. – М.: Книжный мир, 2009. – С. 27.

19) DUO [Электронный ресурс]. – URL: https://www.duosecurity.com/ (дата обращения: 08.10.2015). Загл. с экрана. Яз.рус.

20) Fingerprint Readers [Электронный ресурс] / Bayometric [Электронный ресурс]. – URL: http:// www.bayometric.com/fingerprint-readers.html#isPage=1 (дата обращения: 06.12.2015). Загл. с экрана. Яз.рус.

21) Rohos Logon Key [Электронный ресурс] / Rohos [Электронный ресурс]. – URL: http://www.rohos.ru/products/ rohos-logon-key/ (дата обращения: 07.10.2015). Загл. с экрана. Яз.рус.

22) SecuGen [Электронный ресурс]. – URL: http://www.secugen.com (дата обращения: 06.12.2015). Загл. с экрана. Яз.рус.

23) USB-токены аутентификации с использованием PKI на основе сертификатов [Электронный ресурс] / SafeNet [Элетронный ресурс]. – URL:

http://ru.safenet-inc.com/multi-factor-authentication/authenticators/pki-usb-authentication (дата обращения: 07.10.2015). Загл. с экрана. Яз.рус.

24) Yubikey в России [Электронный ресурс] / Yubico [Электронный ресурс]. – URL: http://www.yubico.ru/ (дата обращения: 07.10.2015). Загл. с экрана. Яз.рус.