Тип работы: Дипломная работа

Предмет: Программирование

Введение

Развитие информационных и коммуникационных технологий в настоящее время создает множество возможностей для синтеза комплексных систем защиты информации важнейшим элементом (подсистемой) которых являются системы авторизации. Системы данного класса позволяют с высокой степенью надежности автоматизировать процесс распознавания объектов – идентификацию, - путем ввода пары логин-пароль, сверки, либо биометрической информации, либо идентификаторов другого типа с имеющимся в базе перечнем разрешенных идентификаторов.
В рамках поставленной цели проведено исследование использования систем NFCдля авторизации в операционных системах и прикладных программах.
Целью выпускной квалификационной работы– создание проекта внедрения системы авторизации в информационных ресурсах с использованием технологии NFC.
Задачи исследования:
- анализ основных принципов авторизации в системе;
- исследование специфики защищаемых объектов в современных условиях;
- анализобщих подходов к построению технологий авторизации;
- сравнительный анализ алгоритмов и технологий аутентификации;
- анализ архитектуры и функционала программного обеспечения, используемого в системах авторизации;
- анализ рисков нарушения работы системы;
- проведение настройки системы для использования аутентификации с использованием NFC.
Объект исследования - системы аутентификации в операционных системах.
Предмет исследования - методика авторизации в информационных системах с использованием технологии NFC
Методы исследования: анализ литературных источников, системный анализ и синтез, моделирование, обобщение, наблюдение.
Гипотеза исследования: внедрение системы авторизации с использованием технологии NFC позволит повысить уровень защитыинформационных ресурсов предприятия, сократить убытки, обусловленные возникновением инцидентов, связанных с информационной безопасностью.

1.Теоретическая часть
1.1. Общие принципы организации технологий аутентификации пользователей

Аутентификация является основой безопасности любой системы на программном уровне. Доступ к данным защищается посредством использования идентификатора и пароля.Таким образом, пользователю, проходящему регистрацию на сервере или в любой другой системе, присваивается уникальный id. Данный идентификатор имеется только у него (это цифровое значение, которое может быть обычным порядковым номером). Идентификация – это представление пользователем данных, а аутентификация – принятие данной информации на стороне сервера. Эти две процедуры и условия их выполнения связаны друг с другом [1].
Идентификатор пользователяпредставляет собой некоторое уникальное количество информации, которая позволяет проводить различиемежду индивидуальными пользователями парольной системы. Зачастую идентификаторы также называют "именем пользователей" (логин) или именем учетной записи пользователей.
Пароль пользователяпредставляет собой некоторое секретное количество данных, известных только пользователям и парольной системе, которые могут быть запомнены пользователями и предъявленыпри прохождении процедуры аутентификации. Одноразовый пароль предоставляетразовую возможность пользователю для прохождения аутентификации. Многоразовый пароль может несколько раз использоваться для проверки подлинности.
Учетная запись пользователяпредставляет собой совокупность его идентификатора и его пароля.
База данных пользователей парольной системы содержит данные учетных записей для всех пользователей данной парольной системы.
Парольнаясистемапредставляет собой программно-аппаратный комплекс, реализующий технологии идентификации и аутентификации пользователей информационно системы на основе работы с одноразовыми или многоразовыми паролями. Как правило, функционирование такого комплексапроизводится совместно с подсистемами разграничения доступа и регистрации событий. В некоторых случаях парольная система может исполнять ряд дополнительных функций, в частности функций генерации и распределения кратковременных криптографических ключей.
Основными задачами проведения аутентификации пользователей в системе являются [3]:
- защита информационных ресурсов автоматизированной системы предприятия от несанкционированного доступа;
- определение подлинности учетной записи пользователя и назначение ей соответствующих прав;
- применение политики для соответствующего уровня доступа авторизовавшегося пользователя.
Основными видами аутентификации считаются [1]:
- Информационная компонента;
- предмет или средство;
- биометрическое устройство;
- пользовательская информация.
Вход под паролем предполагает аутентификацию пользователя в рамках использования информационного ресурса, соответственно пользователь несет ответственность за сохранность в тайне парольной информации.
По функциональному назначению вход в систему посредством использования пароля, как правило, применяется для контроля загрузки системы, контроля функционирования, с целью блокировки и контроля доступа. Для ввода пароля может применяться как клавиатура, так и более современные методы, например, технологии голосового набора или интерактивного набора пароля.
В целях контроля загрузки может проводиться процедура идентификации и аутентификации пользователя перед запуском системы, например, через встроенные средства BIOS. В данном случае выполнение загрузки системы может производиться только санкционированными пользователями.
Идентификация служит для сопоставления каждому пользователю (группе пользователей) соответствующей ему разграничительной политики доступа на защищаемом объекте. Для этого необходимо проведениеидентификации пользователяв самостоятельном режиме – путем указания своего «имени» (идентификатора). Таким образом проводится проверкана наличие доступа текущего пользователя к системе. И в соответствии с введённым идентификатором для пользователяпроводится сопоставление соответствующих прав доступа.

Рисунок 1 - Схема управления паролями на основе аппаратных аутентификаторов

Аутентификация предполагаетконтроль процедуры идентификации. Для аутентификации пользователянеобходимо введение пароля. Корректность вводимого пароля означает однозначное соответствие между регистрирующимся пользователем и идентифицированным в системе пользователем. На рисунке 2 показана архитектура централизованного управления аутентификацией в системе.

Рисунок 2 - Архитектура централизованного управления аутентификацией в системе

Для решения задачи по контролю функционирования вычислительной системы с использованием пароля производятся работы:

1. Контроль пользовательской учетной записи при доступе в систему. Реализуется с использованием штатных средств операционной системы.
2. Контроль при запуске процессов. Вход в те или иные приложения может также защищаться паролями, установленными как программным способом, так и средствами используемых СУБД.
3. Контроль доступа к локальным ресурсам. Например, при доступе к локальным принтерам и т.д. также могут применяться технологии аутентификации ответственных лиц.
4. Контроль доступа к разделяемым сетевым ресурсам. Реализуется в том числе с использованием штатных средств операционной системы. Например, доступ к ресурсам можно разделить паролем.

В качестве ответных действий на несанкционированные действия пользователей система защиты может блокировать некоторые функции: загрузку системы, доступ в систему, учётные записи пользователей, запуск определённых приложений. Для снятия блокировки необходимо проведение авторизации администратором безопасности или ответственным лицом.

Кроме того, пользователем может самостоятельнопроводиться блокировка доступа к системе и к приложениям, и т.д., для блокировки доступа в систему в его отсутствие. Для разблокировки приложений необходимо провести авторизацию под учетной записью текущего пользователя. При этом администратор безопасности может проводить блокировку учетных записей пользователей для возможности входа в систему в нерабочее время.

Таким образом, рассмотрев основные требования и возможности защиты информации посредством использования парольной защиты можно сделать выводы:

1. В целях контроля процесса загрузки может проводиться установка возможности пользовательского контроля перед началом процесса загрузки системы. Также, пользовательский контроль может производиться при определении способа и при доступе к заданиям режима загрузки.
2. В целях контроля доступа возможно проведение контроля пользователя при доступе в систему. Также может осуществляться контроль учетных записей при запуске процесса и контроль доступа к локальным и сетевым ресурсам.
3. В целях снятия блокировки используются технологии контроля администратором безопасности. Также, пользователь может выставлять блокировку на некоторые приложения и т.д, снятие которой возможно только под учетной записью, которая провела блокировку.

Парольная защита устанавливается на следующих уровнях:

- на уровне BIOS;
- на уровне авторизации при входе в операционную систему;
- на уровне авторизации при входе в сетевые операционные системы;
- на уровне авторизации в приложениях;
- использование пин-кодов при работе с устройствами.

На каждом из уровней авторизации устанавливаются свои требования к сложности пароля и политике их смены.

Политика парольной защиты, используемая в автоматизированных системах организаций, должна соответствовать классу защищенности информационной системы.

Парольная защита включает в себя компоненты:

- организационную;
- документационную;
- технологическую.

Организационная компонента парольной защиты предполагает ряд мер, определяющих ответственность пользователя в рамках использования технологии работы с парольной информацией. Данная компонента включает в себя:

- разработку положения о парольной защите информации на предприятии;
- определение степени ответственности за компрометацию пароля;
- определение информационных ресурсов, подлежащих парольной защите и их актуализация.
В организациях, работающих с большими массивами персональных данных и имеющих сложную архитектуру автоматизированной системы практикуется разработка комплекса документационного обеспечения парольной защиты информации, в который входит комплекс локальных нормативных документов в обрасти парольной защиты информации.
Типовой перечень документационного обеспечения парольной защиты включает в себя [2]:
- приказы об утверждении перечня информационных ресурсов;
- перечни защищаемых информационных ресурсов;
- таблицы разграничения доступа к информационным ресурсам;
- парольные карточки;
- ведомости выдачи парольных карточек;
- акты уничтожения парольной документации.
Применение документационного обеспечения в технологии парольной защиты информации призвано повысить ответственность пользователей за сохранность паролей.
Технологические обеспечение парольной защиты предполагает использование технических и программных средств, обеспечивающих поддержку технологии парольной защиты. К ним относятся:
- парольные менеджеры;
- электронные ключи;
- парольные генераторы и др.
Применение технологических средств парольной защиты предполагается в информационных системах со сложной архитектурой, предполагающих многоуровневую авторизацию.
1.2. Общие подходы к построению технологий аутентификации
Наиболее распространенные технологии аутентификации основаны на использовании многоразовых или одноразовых паролей. При этом технологии парольной защиты вследствие своих особенностей в первую очередь выступают в качестве объектов атак извне.Методы парольной аутентификации включают следующие разновидности[12]:
с использованием хранимых копий;
с использованием проверочных значений;
без проведения непосредственной передачи парольной информации проверяющей стороне;
с использованием паролей для получения криптографических ключей.
К первомувидуметодовотносятся системы аутентификации, которыесвязаны с наличием у обеих сторон копий паролей или их свертки. Для организации таких систем необходимо проведение работ по созданию и поддержке базы данных, содержащей пароли или свертки паролей для всех учётных записей. Недостатком данного метода является то, что при получении доступа злоумышленников кданной базе данных возможно прохождение аутентификации от имени любойучётной записи.
Методы, составляющие вторую разновидность, позволяют обеспечивать более высокийуровень безопасности парольной системы, так как проверочные значения, хотя и имеют зависимость от паролей, не могут быть непосредственно использоваться злоумышленниками для входа в систему.
Также, вход в систему без предоставления для проверяющей стороны каких бы то ни было данных о паролях обеспечивает наибольшее эффективныйуровень защиты. Данный метод гарантирует обеспечение высокого уровня безопасности даже в тех случаях, если отмечаются нарушения в работе проверяющей стороны (например, при внедрении в программу регистрации троянского ПО). Рассмотрим пример реализации системы парольной защиты, основанный на методе доказательства с нулевым разглашением.
В качестве особого подхода в технологии проверки подлинности могут использоваться криптографические системы аутентификации. Данные протоколы позволяют описывать последовательность действий, которые должны совершать стороны для проведения взаимной аутентификации.Такжеданные действия, как правило, сочетаются с генерацией и распределением криптографических ключей для шифрования дальнейшего проведения информационного обмена. Корректностьиспользования протоколов аутентификации следует из свойств примененных в них математических и криптографических алгоритмов и может быть обоснована с помощью математического аппарата.
Традиционные парольные системы являются более простыми и дешевыми для реализации, но менее безопасными, чем системы с использованием криптографических протоколов. Криптографические протоколы позволяют обеспечивать более высокие уровни надежности защиты и позволяют дополнительно

решать задачу распределения ключей. При этом используемые в них технологии могутявляться объектом законодательных ограничений.

В качестве основных компонент систем парольной защиты можно рассматривать[7]:

- пользовательские интерфейсы;
- интерфейсы администраторов;
- модули по сопряжению с другими подсистемами безопасности;
- базы данных, содержащие учетные записи.

Парольные системыявляются "передним краем обороны" всей системы информационной безопасности. Некоторые ее компоненты (в частности, связанные с пользовательскими интерфейсами) могут располагаться в местах, открытых для доступа потенциальным злоумышленникам. Вследствие этого парольная система представляет собой главный объект атаки при вторжении злоумышленников в защищенную систему. Далее перечислены виды угроз безопасности, связанные с работой парольных систем.

Разглашение настроек учетных записей через проведение

- подбора в интерактивном режиме
- подсматривания
- проведение преднамеренной передачи пароля его владельцами другим лицам
- получение доступа к базе данных парольной системы
- проведение перехвата переданных по сети данных о пароле
- хранение паролей в доступных местах
- Вмешательство в работу компонентов парольной системы посредством:
- внедрения программных закладок
- обнаружения и использования ошибок, допущенных на стадии разработки
- выведения из строя парольной системы

Некоторые из указанных типов угроз связаны с влиянием человеческого фактора, проявляющегося в том, что для пользователястановятся доступными режимы:

- выбора пароля, который легко запоминается и также легко может быть подобран;
- записи пароля, который сложно запоминается, при хранении записи в доступном месте;
- введение пароля таким образом, что его смогут увидеть посторонние
- передача пароля другим лицам намеренно или под влиянием заблуждения

В дополнение к выше сказанному, необходимо отметить влияние "парадокса человеческого фактора". Данный парадоксзаключается в том, что пользователизачастую стремятся выступать скорее противниками парольной системы, как, впрочем, и любой системы защиты, функционирование которой негативно влияет на его рабочие условия, нежели в качестве союзников системы защиты, тем самым увеличивая степень уязвимости. Защита от указанных угроз основывается на ряде перечисленных ниже организационно-технических мер и мероприятий.

В большинстве систем пользователи имеют возможности самостоятельного выбора паролей, либополучают их от администраторов безопасности. При этом для снижения степени влияния описанного выше человеческого фактора необходима реализация ряда требований к выбору и использованию паролей. В таблице 1 приведено описание основных требований к парольной защите.

Таблица 1 - Перечень основных требований к парольной защите

Требование к выбору паролей	Ожидаемый эффект
Установка минимального количества символов в пароле	Усложнение задачи злоумышленников при попытке подсмотра паролей или подбора паролей с помощью методов "тотального опробования"
Использование в паролях различных групп символов	Усложнение задачи злоумышленника при попытках подбора паролей методом "тотального опробования"
Анализ сложности паролей посредством словарей(исключение чрезмерно простых паролей)	Увеличение времени переборапарольных комбинаций
Установка максимального периода действия пароля	Усложнение задачи злоумышленников по подбору паролей через тотальное опробование, в том числе без проведение непосредственного обращения к системе защиты
Установка минимального срока действия пароля	Препятствует попыткам пользователей замены пароля на старый после его замены по предыдущему требованию
Ведение журнала истории паролей	Обеспечение дополнительной степени защиты по предыдущему требованию

Использование эвристических алгоритмов, бракующих пароли на основании данных журнала истории
Усложнение задачи злоумышленника при попытке подбора пароля по словарю или с использованием эвристических алгоритмов
Ограничение количества попыток ввода пароля Препятствие подбору паролей в интерактивном режиме
Использование процедуры по принудительной смене пароля пользователя Обеспечение эффективности требований, ограничивающих максимальный срок действия пароля
Использование задержки при ошибках аутентификации Препятствие интерактивному подбору паролей злоумышленником
Запрет на самостоятельный выбор паролей и автоматическая генерация паролей Исключение возможности подбора пароль по словарю. При неизвестном алгоритме генерации паролей, подбор возможен только с помощью малоэффективного метода "тотального опробования"
Проведение принудительной смены паролей при первомвходе пользователя в систему Защита от неправомерных действий администраторов, имеющих доступ к паролямпри создании учетной записи
Перечень показателей для проведения количественной оценки стойкости парольных систем приведен в таблице 2.
Таблица 2 - Перечень показателей для проведения количественной оценки стойкости парольных систем

1. ГОСТ Р 51241-2008 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний
2. Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ (ред. от 17.12.2017 №498-ФЗ)
3. Баранников Н. И., Яскевич О. Г. Современные проблемы проектирования корпоративных информационных систем / Н. И. Баранников, О. Г. Яскевич; ФГБОУ ВПО "Воронежский гос. технический ун-т". - Воронеж: Воронежский государственный технический университет, 2014. - 237 с.
4. Михалевич Е.В. Обработка персональных данных: анализ законодательства и судебной практики / Е.В. Михалевич. - Москва: ФГБУ "Редакция "Российской газеты", 2019. - 143 с.
5. Мировой и российский рынок систем биометрии. Прогнозы и тенденции. [Электронный ресурс]. Режим доступа: http://www.techportal.ru/security/biometrics/mirovoy-i-rossiyskiy-rynki-biometrii/#first
6. Ворона В.А., Тихонов В.А. Системы контроля и управления доступом. – М.: Горячая линия - Телеком, 2012. – 272 с.
7. Задорожный, В.Н. Информационные технологии и автоматизация управления. - Омск : Изд-во ОмГТУ, 2016. - 269 с.
8. Идентификация по смартфону - URL: https://www.aamsystems.ru/mobile-access/ (дата обращения: 20.02.2021)
9. V.D. Cunsolo, S. Distefano, A. Puliafito and M.L. Scarpa, ’’Achieving Information Security in Network Computing Systems”, 8th IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009.
10. Горев А. И., Симаков А. А. Обработка и защита информации в компьютерных системах: учебно-практическое пособие / А. И. Горев, А. А. Симаков. - Омск :ОмА МВД России, 2016. - 87 с.
11. Калачев А. Для мобильных стражей: беспроводной стандарт Bluetooth Low Energy в системах безопасности - URL: https://www.compel.ru/lib/ne/2013/1/3-dlya-mobilnyih-strazhey-besprovodnoy-standart-bluetooth-low-energy-v-sistemah-bezopasnosti (дата обращения: 20.06.2019)
12. Крахмалев А.К. Средства и системы контроля и управления доступом. Учебное пособие. М.: НИЦ «Охрана» ГУВО МВД России,2011.
13. Мировой рынок СКУД http://www.techportal.ru/access-control/market/
14. Михайлова Е. М., Анурьева М. С. Организационная защита информации [Электронный ресурс]/ Михайлова Е. М., Анурьева М. С. - Тамбов: ФГБОУ ВО "Тамбовский государственный университет имени Г. Р. Державина", 2017.
15. Мобильная идентификация. Технологии. Чек-лист по выбору системы. Обзор решений. URL: http://www.techportal.ru/review/mobile-access/how-to-choose/ (дата обращения: 20.06.2019)
16. Обзор российского рынка СКУД http://www.s-director.ru/i/tree/101/7_2010.1.pdf
17. Рынок СКУД. URL: http://sio.su/ (дата обращения: 06.06.2019)
18. Системы безопасности http://www.bolid.ru/soft/object/object_5.html
19. Сравнение СКУД. URL: http://biometricsecurity.ru/ (дата обращения: 10.06.2019).
20. J. Harauz, L.M. Kaufman and B. Potter, ”Data Security in the World of Cloud Computing”, IEEE Security and Privacy, 2009.
21. C. Wang, Q. Wang, K. Ren and W. Lou, ’’Privacy-Preserving Public Auditing for Data Storage Security in Could

Computing”, Proceedings of IEEE INFOCOM, 2010.
22. Такатлы Д. А. Защита персональных данных / Д. А. Такатлы. - Петропавловск-Камчатский: Дальневосточный филиал Федерального государственного бюджетного образовательного учреждения высшего образования "Всероссийская академия внешней торговли Министерства экономического развития Российской Федерации", 2016. - 92 с.
23. Melnyk A. O. Multilevel base platform of cyber-physics systems // Cyber-physical systems: achievements and challenges // Materials of the first scientific seminar, Lviv, 2015. – P. 5–15.
24. Jason R. Indoor WiFi Location and Beacons: Better Together. URL: http://blogs.cisco.com/ wireless/ indoor-wifi-location-and-beacons-better-together/ (датаобращения: 10.02.2021).
25. Базовые характеристики СКУД. URL: https://www.inarm.ru/solutions/skud (дата обращения: 28.02.2021)
26. Официальный сайт ФСТЭК России [Электронный ресурс] / Банк данных угроз безопасности информации – Режим доступа: http://bdu.fstec.ru/threat / Дата обращения: 09.02.2021 г.
27. Официальный сайт ФСТЭК России [Электронный ресурс] / Руководящий документ Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации – Режим доступа: https://fstec.ru/component/attachments/download/296 / Дата обращения: 09.02.2021 г.
28. Аникин Д. В. Информационная безопасность и защита информации: учебное пособие / Д.В. Аникин. - Барнаул: Изд-во Алтайского государственного университета, 2018. - 196 с.
29. Ахметов И. В., Карабельская И. В., Губайдуллин И. М., Сафин Р. Р. Моделирование бизнес-процессов: учебное пособие. - Уфа: Уфимский государственный университет экономики и сервиса, 2015. - 67 с.
30. Бабиева Н. А., Раскин Л. И. Проектирование информационных систем: учебно-методическое пособие / Н. А. Бабиева, Л. И. Раскин. - Казань: Медицина, 2014. – 200с.
31. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации / Е. К. Баранова, А. В. Бабаш. - Москва: РИОР ИНФРА-М, 2018. – 334 с.