МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

КУРГАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Кафедра «Безопасность информационных и автоматизированных систем»

РАЗРАБОТКА ПРОГРАММЫ РАЗГРАНИЧЕНИЯ ПОЛНОМОЧИЙ ПОЛЬЗОВАТЕЛЕЙ НА ОСНОВЕ ПАРОЛЬНОЙ АУТЕНТИФИКАЦИИ

Методические указания
к выполнению лабораторной работы
по дисциплине «Теоретические основы компьютерной безопасности»
для студентов направления 090100 специальности 090105

Курган 2011

Кафедра: «Безопасность информационных и автоматизированных систем»

Дисциплина: «Теоретические основы компьютерной безопасности» (направление 095100, специальность 090105)

Составил: ст. преподаватель: В.В. Москвин

Утверждены на заседании кафедры « 25 » ноября 2010 г.

Рекомендованы методическим советом университета « 10 » декабря 2010 г.

ЦЕЛЬ РАБОТЫ

Изучить парольные системы защиты от НСД и научиться программно удалять и добавлять пользователей с заданием привилегий и пароля.

ПРИБОРЫ, ОБОРУДОВАНИЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

1 Операционная система (по выбору).
2 Используемая среда программирования (по выбору).

ТЕОРЕТИЧЕСКОЕ ВВЕДЕНИЕ

Парольные системы для защиты от несанкционированного доступа к информации. Под несанкционированным доступом к информации (НСД) согласно руководящим документам Гостехкомиссии будем понимать доступ к информации, нарушающий установленные правила разграничения доступа и осуществляемый с использованием штатных средств, предоставляемых СВТ или АС.

Рассмотрим подробнее такие технологические методы защиты от НСД, как идентификация, аутентификация и используемое при их реализации криптографическое преобразование информации.

Идентификация - это присвоение пользователям идентификаторов и проверка предъявляемых идентификаторов по списку присвоенных.

Аутентификация - это проверка принадлежности пользователю предъявленного им идентификатора. Часто аутентификацию также называют подтверждением или проверкой подлинности.

Под **безопасностью (стойкостью)** системы идентификации и аутентификации будем понимать степень обеспечиваемых ею гарантий того, что злоумышленник не способен пройти аутентификацию от имени другого пользователя. В этом смысле, чем выше стойкость системы аутентификации, тем сложнее злоумышленнику решить указанную задачу. Система идентификации и аутентификации является одним из ключевых элементов инфраструктуры защиты от НСД любой информационной системы. Различают три группы методов аутентификации, основанных на наличии у каждого пользователя:

- индивидуального объекта заданного типа;
- знаний некоторой известной только ему и проверяющей стороне информации;
- индивидуальных биометрических характеристик.

К первой группе относятся методы аутентификации, использующие удостоверения, пропуска, магнитные карты и другие носимые устройства, которые широко применяются для контроля доступа в помещения, а также входят в состав программно-аппаратных комплексов защиты от НСД к средствам вычислительной техники.

Во вторую группу входят методы аутентификации, использующие пароли. По экономическим причинам они включаются в качестве базовых средств защиты во многие программно-аппаратные комплексы защиты информации. Все современные операционные системы и многие приложения имеют встроенные механизмы парольной защиты.

Последнюю группу составляют методы аутентификации, основанные на применении оборудования для измерения и сравнения с эталоном заданных индивидуальных характеристик пользователя: тембра голоса, отпечатков пальцев, структуры радужной оболочки глаза и др. Такие средства позволяют с высокой точностью аутентифицировать обладателя конкретного биометрического признака, причем «подделать» биометрические параметры практически невозможно. Однако широкое распространение подобных технологий сдерживается высокой стоимостью необходимого оборудования.

Если в процедуре аутентификации участвуют только две стороны, устанавливающие подлинность друг друга, такая процедура называется *непосредственной аутентификацией* (**direct password authentication**). Если же в процессе аутентификации участвуют не только эти стороны, но и другие, вспомогательные, говорят об *аутентификации с участием доверенной стороны* (**trusted third party authentication**). При этом третью сторону называют *сервером аутентификации* (**authentication serve**r) или *арбитратором* (**arbitrator**).

Общие подходы к построению парольных систем. Наиболее распространенные методы аутентификации основаны на применении многоразовых или одноразовых паролей. Эти методы включают следующие разновидности способов аутентификации:

• по хранимой копии пароля или его свёртке (plaintext-equivalent);

• по некоторому проверочному значению (verifier-based);

• без непосредственной передачи информации о пароле проверяющей стороне

(zero-knowledge);

• с использованием пароля для получения криптографического ключа

(cryptographic).

В первую разновидность способов входят системы аутентификации, предполагающие наличие у обеих сторон копии пароля или его свертки. Для организации таких систем требуется создать и поддерживать базу данных, содержащую пароли или сверки паролей всех пользователей. Их слабой стороной является то, что получение злоумышленником этой базы данных позволяет ему проходить аутентификацию от имени любого пользователя.

Способы, составляющие вторую разновидность, обеспечивают более высокую степень безопасности парольной системы, так как проверочные значения, хотя они и зависят от паролей, не могут быть непосредственно использованы злоумышленником для аутентификации.

Аутентификация без предоставления проверяющей стороне какой бы то ни было информации о пароле обеспечивает наибольшую степень защиты. Этот способ гарантирует безопасность даже в том случае, если нарушена работа

проверяющей стороны (например, в программу регистрации в системе внедрен «троянский конь»). По данному принципу построена система парольной защиты на базе «доказательства с нулевым разглашением».

Особым подходом в технологии проверки подлинности являются криптографические протоколы аутентификации. Такие протоколы описывают последовательность действий, которую должны совершить стороны для взаимной аутентификации, кроме того, эти действия, как правило, сочетаются с генерацией и распределением криптографических ключей для шифрования последующего информационного обмена. Корректность протоколов аутентификации вытекает из свойств задействованных в них математических и криптографических преобразований и может быть строго доказана.

Обычные парольные системы проще и дешевле для реализации, но менее безопасны, чем системы с криптографическими протоколами. Последние обеспечивают более надежную защиту и дополнительно решают задачу распределения ключей. Однако используемые в них технологии могут быть объектом законодательных ограничений.

Для более детального рассмотрения принципов построения парольных систем сформулируем несколько основных определений.

Идентификатор пользователя - некоторое уникальное количество информации, позволяющее различать индивидуальных пользователей парольной системы (проводить их идентификацию). Часто идентификатор также называют именем пользователя или именем учетной записи пользователя.

Пароль пользователя - некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации. Одноразовый пароль дает возможность пользователю однократно пройти аутентификацию. Многоразовый пароль может быть использован для проверки подлинности повторно.

Учетная запись пользователя - совокупность его идентификатора и его пароля. База данных пользователей парольной системы содержит учетные записи всех пользователей данной парольной системы.

Под **парольной системой** будем понимать программно-аппаратный комплекс, реализующий системы идентификации и аутентификации пользователей АС на основе одноразовых или многоразовых паролей. Как правило, такой комплекс функционирует совместно с подсистемами разграничения доступа и регистрации событий. В отдельных случаях парольная система может выполнять ряд дополнительных функций, в частности генерацию и распределение кратковременных (сеансовых) криптографических ключей.

Основными компонентами парольной системы являются:

- интерфейс пользователя;
- интерфейс администратора;
- модуль сопряжения с другими подсистемами безопасности;
- база данных учетных записей.

Парольная система представляет собой «передний край обороны» всей системы безопасности. Некоторые ее элементы (в частности, реализующие интерфейс пользователя) могут быть расположены в местах, открытых для доступа потенциальному злоумышленнику. Поэтому парольная система становится одним из первых объектов атаки при вторжении злоумышленника в защищенную систему.

Возможны следующие типы угроз безопасности парольных систем:

1 Разглашение параметров учетной записи через:

• подбор в интерактивном режиме;

• подсматривание;

• преднамеренную передачу пароля его владельцем другому лицу;

• захват базы данных парольной системы (если пароли не хранятся в базе в открытом виде, для их восстановления может потребоваться подбор или дешифрование);

• перехват переданной по сети информации о пароле;

• хранение пароля в доступном месте.

2 Вмешательство в функционирование компонентов парольной системы через:

• внедрение программных закладок;

• обнаружение и использование ошибок, допущенных на стадии разработки;

• выведение из строя парольной системы.

Некоторые из перечисленных типов угроз связаны с наличием так называемого человеческого фактора, проявляющегося в том, что пользователь может:

• выбрать пароль, который легко запомнить и также легко подобрать;

• записать пароль, который сложно запомнить, и положить запись в доступном

месте;

• ввести пароль так, что его смогут увидеть посторонние;

• передать пароль другому лицу намеренно или под влиянием заблуждения.

Кроме того, необходимо отметить существование «парадокса человеческого фактора». Заключается он в том, что пользователь нередко стремится выступать скорее противником парольной системы, как, впрочем, и любой системы безопасности, функционирование которой влияет на его рабочие условия, нежели союзником системы защиты, тем самым ослабляя ее. Защита от указанных угроз основывается на ряде перечисленных ниже организационно-технических мер и мероприятий.

Требования к парольным системам защиты от НСД. В большинстве систем пользователи имеют возможность самостоятельно выбирать пароли или получают их от системных администраторов. При этом для уменьшения деструктивного влияния описанного выше человеческого фактора необходимо реализовать ряд требований к выбору и использованию паролей (таблица 1).

Таблица 1- **Требования к выбору и использованию паролей**

Требования к выбору пароля	Получаемый эффект
Установление минимальной длины пароля	Усложняет задачу злоумышленника при попытке подсмотреть пароль или подобрать пароль методом «тотального опробования»
Использование в пароле различных групп символов	Усложняет задачу злоумышленника при попытке подобрать пароль методом «тотального опробования»
Проверка и отбраковка пароля по словарю	Усложняет задачу злоумышленника при попытке подобрать пароль по словарю
Установление максимального срока действия пароля	Усложняет задачу злоумышленника по подбору паролей методом тотального опробования, в том числе без непосредственного обращения к системе защиты (режим off-line)
Установление минимального срока действия пароля	Заменить пароль на старый после его смены по предыдущему требованию
Ведение журнала истории паролей	Обеспечивает дополнительную степень защиты по предыдущему требованию
Применение эвристического алгоритма, бракующего пароли на основании данных журнала	Добрать пароль по словарю или с использованием эвристического алгоритма
Ограничение числа попыток ввода пароля	Препятствует интерактивному подбору паролей злоумышленником
Поддержка режима принудительной смены пароля пользователя	Обеспечивает эффективность требования, ограничивающего максимальный срок действия пароля
Использование задержки при вводе неправильного пароля	Препятствует интерактивному подбору паролей злоумышленником
Запрет на выбор пароля самим пользователем и автоматическая генерация паролей	Исключает возможность подобрать пароль по словарю. Если алгоритм генерации паролей не известен злоумышленнику, последний может подбирать пароли только методом «тотального опробования»
Принудительная смена пароля при первой регистрации пользователя в системе	Защищает от неправомерных действий системного администратора, имеющего доступ к паролю в момент создания учетной записи

Для количественной оценки стойкости парольных систем вводится несколько взаимосвязанных параметров (таблица 2).

Таблица 2- **Параметры стойкости парольной системы**

Параметр	Способ определения
Мощность алфавита паролей ***A***	Могут варьироваться для обеспечения заданного значения ***S*** ***(S=A^L)***
Длина пароля ***L***	
Мощность пространства паролей ***S***	Вычисляется на основе заданных значений ***P***, ***T*** или ***V***
Скорость подбора паролей ***V:*** • Для интерактивного режима определяется как скорость обработки одной попытки регистрации проверяющей стороной. • Для режима off-line (на основе свертки пароля) определяется как скорость вычисления значения свертки для одного пробного пароля	Может быть искусственно увеличена для защиты от данной угрозы Задается используемым алгоритмом вычисления свертки. Алгоритм, имеющий медленные реализации, повышает стойкость по отношению к данной угрозе
Срок действия пароля (задает промежуток времени, по истечении которого пароль должен быть обязательно сменен) ***T***	Определяется исходя из заданной вероятности ***P***, или полагается заданным для дальнейшего определения ***S***
Вероятность подбора пароля в течение его срока действия (подбор продолжается непрерывно в течение всего срока действия пароля) ***P***	Выбирается заранее для дальнейшего определения ***S*** или ***T***

Порядок выполнения работы

1 Выбрать операционную систему.

2 Выбрать язык и соответствующую среду программирования.

3 Получить вариант индивидуального задания у преподавателя.

4 Разработать программу, удовлетворяющую нижеперечисленным условиям:

а) программа должна обеспечивать работу режиме администратора (пользователя с фиксированным именем ADMIN).

б) в режиме администратора программа должна поддерживать следующие функции (при правильном вводе пароля):

- смена пароля администратора (при правильном вводе старого пароля);
- просмотр списка имен зарегистрированных пользователей и установленных для них параметров (принадлежность к группам, блокировка учетной записи, включение ограничений на выбираемые пароли) – всего списка целиком в одном окне или по одному элементу

списка с возможностью перемещения к его началу или концу;

- создание нового пользователя с уникальным именем, паролем и привилегиями;
- блокирование возможности работы пользователя с заданным именем;
- включение или отключение ограничений на выбираемые пользователем
  пароли (в соответствии с индивидуальным заданием, определяемым номером варианта);
- удаление пользователя с заданным именем;
- завершение работы с программой.

5 В режиме обычного пользователя изменять его пароль и завершать работу программы, остальные ее функции должны быть заблокированы.

6 После своего запуска программа должна вывести интерфейс с окном для ввода имени пользователя, пароля пользователя. При вводе пароля его символы на экране всегда должны заменяться символом ‘*’ (при создании или изменении пароля данная функция может быть опциональной).

7 При отсутствии введенного в окне входа имени пользователя в списке зарегистрированных администратором пользователей программа должна выдавать соответствующее сообщение и предоставлять пользователю возможность повторного ввода имени или завершения работы с программой.

8 При неправильном вводе пароля в окне входа программа должна выдавать соответствующее сообщение и предоставлять пользователю возможность повторного ввода. При трехкратном вводе неверного пароля работа программы должна завершаться.

9 При первоначальном вводе пароля (обязательном при первом входе администратора или пользователя с зарегистрированным ранее администратором именем) и при дальнейшей замене пароля программа должна просить пользователя подтвердить введенный пароль путем его повторного ввода.

10 При попытке создания уже имеющегося в списке имени пользователя программа должна выдавать соответствующее сообщение и предоставлять пользователю возможность повторного ввода имени или завершения работы с программой.

11 Если выбранный пользователем пароль не соответствует требуемым ограничениям (при установке соответствующего параметра учетной записи пользователя), то программа должна выдавать соответствующее сообщение и предоставлять пользователю возможность ввода другого пароля, завершения работы с программой или отказа от смены пароля.

12 Интерфейс с программой должен быть организован на основе меню, обязательной частью которого должно являться подменю «Справка» с командой «О программе». При выборе этой команды должна выдаваться информация об авторе программы и выданном индивидуальном задании. Интерфейс пользователя программы может также включать панель управления с дублирующими команды меню графическими кнопками и строку состояния.

13 Для реализации указанных в пункте 2 функций в программе должны использоваться специальные диалоговые формы, позволяющие администратору вводить необходимую информацию.

Возможный вид диалоговых форм программы (рисунок 1).

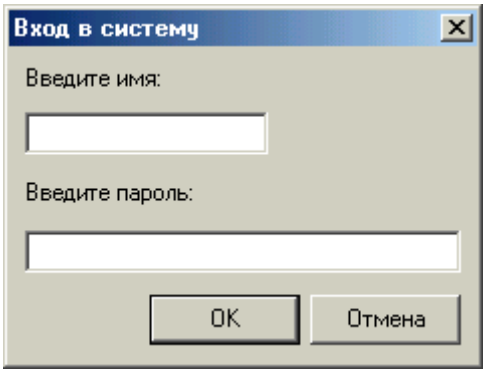

Рисунок 1 - Окно входа в программу

Может быть создано на основе шаблона Password Dialog, выбираемого с помощью команды File | New | Dialogs систем программирования Borland Delphi или Borland C++ Builder (рисунок 2).

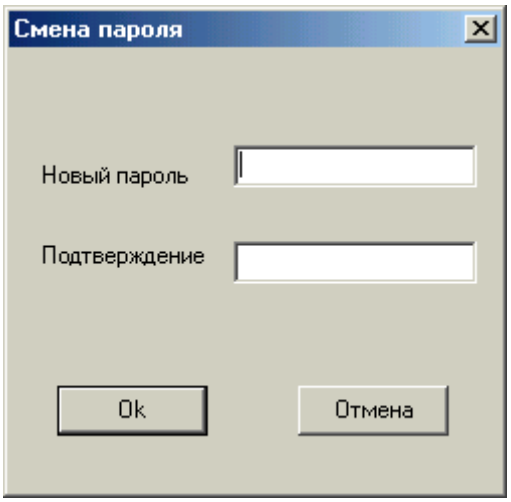

Рисунок 2 - Окно смены пароля

Возможно добавление на форму надписи «Старый пароль» и редактируемой строки для ввода действующего пароля (рисунок 3).

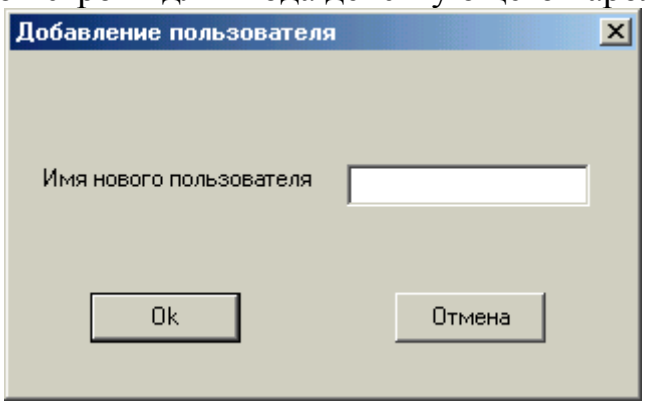

Рисунок 3 - Окно добавление нового пользователя

Возможно добавление на форму элементов управления для отображения и изменения значений параметров, устанавливаемых администратором для новой учетной записи (блокировка, ограничение на выбираемые пароли). Рисунок 4.

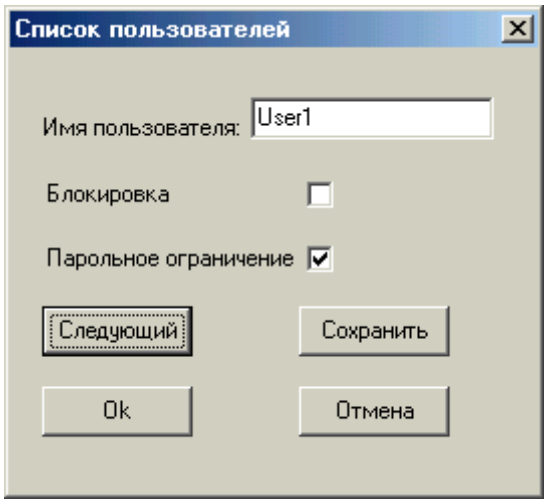

Рисунок 4 - Окно просмотра (редактирования) учетных записей

Возможно добавление кнопки «Предыдущий» для перехода к предыдущей учетной записи или отображение списка учетных записей пользователей и их параметров в одном окне с помощью компонента StringGrid (группа Additional) систем программирования Borland Delphi или Borland C++ Builder.

14 Для реализации указанных в пунктах 2-3 функций в программе должны использоваться специальные диалоговые формы, позволяющие администратору вводить необходимую информацию.

15 Представить отчет по выполненной работе с блок-схемой программы и описанием использованных в ней алгоритмов. Приложить zip-архив с исходным и исполняемым кодом разработанной программы.

Индивидуальные варианты заданий (ограничения на выбираемые пароли)

1 Длина не меньше минимальной длины, устанавливаемой администратором и сохраняемой в учетной записи пользователя.
2 Наличие строчных и прописных букв.
3 Наличие букв и цифр.
4 Наличие букв и знаков препинания.
5 Наличие цифр и знаков препинания.
6 Наличие букв и знаков арифметических операций.
7 Наличие цифр и знаков арифметических операций.
8 Наличие латинских букв и символов кириллицы.
9 Наличие букв, цифр и знаков препинания.
10 Наличие латинских букв, символов кириллицы и цифр.
11 Наличие латинских букв, символов кириллицы и знаков препинания.
12 Наличие строчных и прописных букв, а также цифр.
13 Наличие строчных и прописных букв, а также знаков препинания.
14 Наличие строчных и прописных букв, а также знаков арифметических операций.
15 Наличие латинских букв, символов кириллицы и знаков арифметических операций.
16 Наличие букв, цифр и знаков арифметических операций.
17 Наличие букв, знаков препинания и знаков арифметических операций.
18 Наличие цифр, знаков препинания и знаков арифметических операций.
19 Отсутствие повторяющихся символов.
20 Чередование букв, цифр и снова букв.
21 Чередование букв, знаков препинания и снова букв.
22 Чередование цифр, букв и снова цифр.
23 Отсутствие подряд расположенных одинаковых символов.
24 Чередование цифр, знаков препинания и снова цифр.
25 Чередование цифр, знаков арифметических операций и снова цифр.
26 Несовпадение с именем пользователя.
27 Несовпадение с именем пользователя, записанным в обратном порядке.
28 Наличие строчных и прописных букв, цифр и знаков препинания.
29 Наличие строчных и прописных букв, цифр и знаков арифметических операций.
30 Несовпадение с датой в одном из форматов: дд/мм/гг, дд-мм-гг, дд.мм.гг.

Контрольные вопросы

1 Способы аутентификации пользователей в компьютерных системах.
2 Организация базы учетных записей пользователей и доступа к ней.
3 Хранение идентифицирующей информации в операционной системе Unix.
4 Хранение идентифицирующей информации в операционной системе Windows.
5 Аутентификация пользователей на основе паролей.
6 Использование одноразовых паролей.
7 Аутентификация пользователей на основе модели «рукопожатия».
8 Аутентификация пользователей по их биометрическим характеристикам.
9 Разграничение прав пользователей в незащищенных версиях ОС Windows.
10 Разграничение прав субъектов в защищенных версиях ОС Windows.

Список литературы

1 Хатч Б., Ли Д., Курц Д. Секреты хакеров. Безопасность Linux – готовые решения/Пер. с англ. – М.: Вильямс, 2004.
2 Скембрей Д., Мак-Клар С. Секреты хакеров. Безопасность Windows 2000 – готовые решения/Пер. с англ. – М.: Вильямс, 2002.
3 Грушо А.А., Применко Э.А., Тимонина Е.Е. Теоретические основы компьютерной безопасности. – М.: Академия, 2009.

Москвин Владимир Викторович

РАЗРАБОТКА ПРОГРАММЫ РАЗГРАНИЧЕНИЯ ПОЛНОМОЧИЙ ПОЛЬЗОВАТЕЛЕЙ НА ОСНОВЕ ПАРОЛЬНОЙ АУТЕНТИФИКАЦИИ

Методические указания
к выполнению лабораторной работы
по дисциплине «Теоретические основы компьютерной безопасности»
для студентов направления 095100
специальности 090105

Подписано к печати	Формат 60×84 1/16	Бумага тип. №1
Печать трафаретная	Усл. печ.л. 1	Уч.-изд.л.1
Заказ	Тираж э/в	Цена свободная

РИЦ Курганского государственного университета
640669, г. Курган, ул. Гоголя,25
Курганский государственный университет