УДК 004.056.53

**Анализ алгоритма аутентификации подключаемых модулей аутентификации**

*А.С.Васильев С.В. Керш*

*phpmaster07@gmail.com*

Омский государственный технический университет

UDC 004.056.53

**Analysis of the algorithm Pluggable Authentication Modules**

*A.S.Vasilev S.V. Kersh*

*phpmaster07@gmail.com*

OmskStateTechnicalUniversity

*Объектом исследования является аутентификация пользователя. Предметом исследования являются подключаемые модули аутентификации.*

*Цель работы заключается в повышении качества защиты путем создания собственного подключаемого модуля аутентификации.*

*В процессе работы проводились теоретические исследования способом аутентификации.*

*В результате работы был создан подключаемый модуль аутентификации, который повысил уровень защиты учетной записи пользователя.*

*Ключевые слова: аутентификация, PAM, пользователь, логин, учетная запись, операционная система, библиотека.*

*The object of the study is user authentication. The subject of the study are the PAM-modules.*

*The purpose of the work is to improve the quality of protection by creating their own PAM-modul.*

*In the process, we carried out theoretical studies of authentication methods.*

*As a result, the work was created by the PAM-modul, which raised the level of protection of the user account.*

*Keywords: authentication , PAM, user, login, account, operating system, library.*

Мир, в котором мы живем, и передовые технологии постоянно улучшаются, поэтому не стоит пренебрегать такой основой любой жизни, как безопасность. В реальной жизни, люди узнают друг друга в лицо, по паспорту и т.д. Распознать человека, сидящего за компьютером, для системы, намного сложнее – это требует необычных методов.

Перед тем как проверять пользователя, нужна идентификация, то есть из многих субъектов, зарегистрированных в системе, выбрать по некоторому уникальному идентификатору, одного из них. Идентификатор то система и будет проверять. Идентификатор – это набор символов, имя пользователя, под которым зарегистрирован пользователь в проверяющей его компьютерной системе.

Аутентификация – это проверка подлинности предъявленного пользователем идентификатора.

Аутентификация пользователей всегда производится некоторым программным модулем, принадлежащим компьютеру, к которому пользователь пытается получить доступ. Алгоритм действий данного модуля можно условно разделить на два этапа:

– начальный этап, на котором модуль формирует пароль, по которому пользователь будет распознаваться;

– конечный этап, когда пользователь проходит аутентификацию и у него запрашивается аутентификационная информация, которая сравнивается со сформированным на первом этапе паролем.

Существуют более сложные виды аутентификации, когда предъявляемая пользователем аутентификационная информация и пароль могут дополнять друг друга, участвуя в каких-либо криптографических преобразованиях, либо используется несколько паролей.

В зависимости от ситуации может понадобиться смена алгоритма аутентификации. Например, злоумышленник узнал пароль, или требуется более легкая схема входа в систему.

Для UNIX-подобных операционных систем было найдено решение, были разработаны подключаемые модули аутентификации. Подключаемые модули аутентификации (*Pluggable Authentication Modules*, *PAM*), были разработаны в качестве гибкого средства аутентификации пользователей. Долгие годы под аутентификацией в среде *UNIX* подразумевалось сопоставление регистрационных данных пользователей с их записями в файле. Необходимость в усилении защиты и поддержке большего разнообразия средств аутентификации потребовала более гибкого подхода. Сегодня определенные *PAM* выполняют аутентификацию централизовано, используя глобальные аутентификационные каталоги.

Концепция проста: программам, выполняющим аутентификацию, достаточно «знать» лишь о том, что имеется некий модуль, который проведёт аутентификацию за них. Система конфигурируется таким образом, чтобы модули можно было удалять, добавлять и перенастраивать в любое время. Вовсе не обязательно, чтобы модуль был скомпонован (или даже существовал) на этапе компиляции утилиты. Благодаря этому модули *PAM* стали удобным средством системного администрирования.

Библиотека *PAM* и адаптированное под *PAM* программное обеспечение значительно упрощают проблему аутентификации. С помощью *PAM* возможно использование одной и той же базы данных пользователей для каждого процесса выполняющего вход в систему. Кроме того, возможно использование более чем одного базового механизма аутентификации управляемого через *PAM* и являющегося абсолютно прозрачным для пользователей.

В *PAM* имеется хорошо определённое *API* и программное обеспечение будет нормально работать в случае если системный администратор изменит конфигурацию используемого механизма аутентификации. К тому же, файл паролей не масштабируется. Возможна работа с 100 пользователями, но работа с 5000 пользователей совершенно другая история. С помощью *PAM* с лёгкостью можно увеличить количество пользователей до 10 тысяч, в зависимости от используемой базы данных для хранения пользовательской информации. Разработчики могут использовать преимущества *PAM* в случае, если в приложении должен быть реализован механизм аутентификации. Используя *PAM* для аутентификации получается меньше программного кода в отличии от собственной разработки такого же механизма. Принцип работы заключается в следующих этапах:

– приложение делает первичное обращение к *PAM*;

– *PAM* находит соответствующий конфигурационный файл в каталоге и загружает из него список модулей, необходимых для обслуживания запроса;

– после этого *PAM* загружает модули в том порядке, в котором они перечислены в конфигурационном файле. Не все модули нужно загружать – это зависит от параметров конфигурации;

– некоторые модули организуют диалог с пользователем через вызывающее приложение. В ходе диалога обычно выдаётся приглашение на ввод различных параметров, например пароля. Если предоставленные пользователем данные подходит, управление возвращается *PAM*, который вызывает следующий модуль. В конечном итоге процедура аутентификации заканчивается успехом или неудачей. В случае неудачи выдается обобщенное сообщение об ошибке, которое, как правило, не раскрывает причину такого результата. Это своего рода защитная мера, чтобы злоумышленники, пытающиеся взломать систему, не смогли узнать ничего лишнего. В то же время все модули оснащены средствами журнальной регистрации, что позволяет системным администраторам выявлять источники проблем и попытки нарушения прав доступа.

Учетная запись пользователя является коллекцией информации, которая сообщает операционной системе о файлах и папках, к которым имеет доступ пользователь, какие изменения в компьютере он может выполнять, а также личные настройки, например фон рабочего стола и экранную заставку. Применение учетных записей позволяет нескольким пользователям работать на одном компьютере с использованием собственных файлов и параметров. Для доступа к учетной записи используется имя пользователя и пароль.

Существуют три типа учетных записей. Каждый тип дает пользователю разные возможности для управления компьютером:

– стандартные учетные записи пользователей, предназначены для повседневной работы;

– учетные записи администратора предоставляют полный контроль над компьютером и применяются только в необходимых случаях;

– учетные записи гостя предназначены для временного доступа к компьютеру.

При установке операционной системы потребуется создать учетную запись пользователя. Она будет являться учетной записью администратора, позволяющей настраивать компьютер и устанавливать любые программы. После настройки компьютера для повседневной работы рекомендуется использовать стандартную учетную запись. На экране приветствия, с которого выполняется вход в операционную систему, отображаются доступные на компьютере учетные записи, а также указываются их типы, что позволяет определить, является ли учетная запись стандартной или имеет права администратора.

Применение обычных учетных записей позволяет защитить компьютер, предотвращая внесение изменений, затрагивающих всех пользователей компьютера, например, удаление системных файлов. Рекомендуется создавать стандартную учетную запись для каждого пользователя компьютера.

При входе в операционную систему с использованием обычной учетной записи можно выполнять те же действия, что и с учетной записью администратора, но для внесения изменений, влияющих на всех пользователей компьютера (например, для установки программного обеспечения или изменения параметров безопасности), в операционную систему может запрашиваться пароль администратора.

В некоторых операционных системах возможно создание учетной записи без пароля, однако рекомендуется использовать надежный пароль. Использование пароля очень важно для обеспечения безопасности компьютера. Когда компьютер защищен паролем, только знающий его пользователь может войти в систему

В операционной системе *Ubuntu* по умолчанию установлена аутентификация по многоразовым паролям. Аутентификация по многоразовым паролям является слабой относительно других способов аутентификации.

Будем считать аутентификацию по многоразовым паролем первым уровнем защиты. Так как первый уровень защиты уже реализован, нужно выявить способ, который можно считать вторым уровнем защиты.

При использовании одноразового пароля – пароль действителен только для одного входа в систему, при каждом следующем запросе доступа требуется новый пароль. Реализован механизм аутентификации по одноразовым паролям может быть как аппаратно, так и программно. Этот метод лучше, чем аутентификация по многоразовым паролям, но другим методам он уступает.

Например при аутентификации с помощью *SMS*-сообщений, пароль:

– является одноразовым;

– пароль имеет дополнительный уровень защиты в виде *PIN*-кода мобильного устройства.

Можно сделать вывод, что аутентификация с помощью *SMS*-сообщений лучше, чем аутентификация по одноразовым паролям.

Биометрическая аутентификация основана на индивидуальных особенностях человека.

Ввиду отсутствия таких приборов как сканер сетчатки и отпечатков пальцев, возможно только отслеживание скорости ввода с клавиатуры. Такая аутентификация может быть хуже аутентификации по одноразовым паролям, из-за совпадения скорости ввода субъекта аутентификации и злоумышленника.

Так как многофакторная аутентификация является самой лучшей, выбираем алгоритм с тремя уровнями защиты, которые возможно реализовать без дополнительных устройств:

– первый уровень – аутентификация по динамическому паролю, как альтернатива одноразовым паролям;

– второй уровень – аутентификация по паролю, полученному в результате математических вычислений;

– третий уровень – аутентификация по паролю, зашифрованному в логической игре.

На основе проведенного анализа были рассмотрены и созданы:

1) Подробная инструкция по установке программного обеспечения для создания подключаемого модуля аутентификации.

2) Новый подключаемый модуль аутентификации.

**Библиографический список**

1. Воройский, Ф. С. Информатика. Новый систематизированный толковый словарь-справочник / Ф. С. Воройский. – М. : ФИЗМАТЛИТ, 2003.

2. Классы, интерфейсы и делегаты в С++ 2005 : учебное пособие / сост. О. Н. Евсеева, А. Б. Шамшев. – Ульяновск : УлГТУ, 2008.

3. Установка Ubuntu [Электронный ресурс] / П. В. Ветров, Тюменский государственный университет. Институт математики и компьютерных наук. – Режим доступа: http://help.ubuntu.ru/manual/, свободный. – Загл. с экрана.

**References**

1. Felix , FS Informatics . New Dictionary of systematic catalog / FS Felix . - M. ​​: FIZMATLIT , 2003.

2. Classes , interfaces and delegates in C ++ 2005 : Textbook / Ed. O. Yevseyev , AB Shamshev . - Ulyanovsk: Ulyanovsk State Technical University , 2008 .

3. Installing Ubuntu [ electronic resource] / PV Winds , Tyumen State University . Institute of Mathematics and Computer Science . - Access : http://help.ubuntu.ru/manual/, free . - Caps . from the screen.