**Задание на 28.01.2022**

МДК 03.02 Программно-аппаратные средства защиты информации

1. **Сделать конспект лекции**
2. **Сделать практическую работу №5** Права доступа к элементам файловой системы.
3. **Сделать практическую работу №6** Разработка подсистемы защиты операционной системы Linux.
4. **Отчет отправить на почту svebalch@mail.ru**

**Лекция 6**

**Простая аутентификация**

Одной из распространенных схем аутентификации является *простая аутентификация*, которая основана на применении традиционных многоразовых паролей с одновременным согласованием средств их использования и обработки. Аутентификация на основе многоразовых паролей — простой и наглядный пример использования разделяемой информации.

Пока в большинстве видов защищенных виртуальных сетей VPN доступ клиента к серверу разрешается по паролю. Однако все чаше применяются более эффективные средства, например программные и аппаратные системы аутентификации на основе одноразовых паролей, цифровых сертификатов.

**1. Аутентификация на основе многоразовых паролей**

Базовый принцип «единого входа» предполагает достаточность одноразового прохождения пользователем процедуры аутентификации для доступа ко всем сетевым ресурсам. Поэтому в современных операционных системах предусматривается централизованная служба аутентификации, которая выполняется одним из серверов сети и использует для своей работы базу данных, где хранятся учетные записи пользователей сети. В эти учетные данные наряду с другой информацией включены идентификаторы и пароли пользователей.

Процедуру простой аутентификации пользователя в сети можно представить следующим образом. При попытке логического входа в сеть пользователь набирает на клавиатуре компьютера свои идентификатор и пароль. Эти данные поступают для обработки на сервер аутентификации. В базе данных, хранящейся на сервере аутентификации, по идентификатору пользователя находится соответствующая запись; из нее извлекается пароль и сравнивается с тем паролем, который ввел пользователь. Если они совпали, то аутентификация прошла успешно, пользователь получает легальный статус и те права на ресурсы сети, которые определены для его статуса системой авторизации.

В схеме простой аутентификации передача пароля и идентификатора пользователя может производиться следующими способами

• в незашифрованном виде. Например, согласно протоколу парольной аутентификации РАР (Password Authentication Protocol) пароли передаются по линии связи в открытой незащищенной форме; • в защищенном виде. Все передаваемые данные (идентификатор и пароль пользователя, случайное число и метки времени) защищены посредством шифрования или однонаправленной функции.



Схема простой аутентификации с использованием пароля показана на рис. 7.1. Вариант аутентификации с передачей пароля пользователя в незашифрованном виде не гарантирует даже минимального уровня безопасности, так как процесс подвержен многочисленным атакам и легко компрометируется. Чтобы защитить пароль, его нужно зашифровать перед пересылкой по незащищенному каналу. Для этого в схему включены средства шифрования *Ек* и расшифрования *Dk*, управляемые разделяемым секретным ключом *К*. Проверка подлинности пользователя основана на сравнении присланного пользователем пароля *PA* и исходного значения *РА’* хранящегося в сервере аутентификации. Если значения *PA* и *РА’* совпадают, то пароль *PA* считается подлинным, а пользователь *А* — законным.

Схемы организации простой аутентификации различаются не только методами передачи паролей, но и видами их хранения и проверки. Наиболее распространенный способ — хранение паролей пользователей в открытом виде в системных файлах, причем на эти файлы устанавливаются атрибуты защиты от чтения и записи (например, при помощи описания соответствующих привилегий в списках контроля доступа операционной Системы). Система сопоставляет введенный пользователем пароль с хранящейся в файле паролей записью. В этом случае не используются криптографические механизмы, такие как шифрование или однонаправленные функции. Недостатком данного способа является возможность получения злоумышленником в системе привилегий администратора, включая права доступа к системным файлам, и в частности, к файлу паролей.

С точки зрения безопасности более предпочтителен метод передачи и хранения паролей с использованием односторонних функций. Его суть заключается в том, что пользователь должен пересылать вместо открытой формы пароля его отображение, получаемое с использованием односторонней функции *h* (.). Это преобразование гарантирует невозможность раскрытия противником пароля по его отображению, так как противник наталкивается на неразрешимую числовую задачу.

Например, односторонняя функция *h* (.) может быть определена следующим образом:

, где *Р* — пароль пользователя;

*ID* — идентификатор пользователя;

*Ер* — процедура шифрования, выполняемая с использованием пароля Р в качестве ключа.

Такие функции удобны, если длина пароля и ключа одинаковы. В этом случае проверка подлинности пользователя А с помощью пароля *РА* состоит из пересылки серверу аутентификации отображения *h (РА)* и сравнения его с предварительно вычисленным и хранимым в базе данных сервера аутентификации эквивалентом *h’* (*РА*). Если отображения *h* (*РА*) и *h’* (*РА*) равны, то считается, что пользователь успешно прошел аутентификацию.

На практике пароли состоят лишь из нескольких символов— так пользователям легче запомнить их. Короткие пароли уязвимы к атаке полного перебора всех вариантов. для того чтобы предотвратить подобную атаку, функцию *h (Р)* можно определить иначе, например в виде:

*h (P)= E рек (ID)*,

где *К* и *ID* — соответственно ключ и идентификатор отправителя.

Различают две формы представления объектов, аутентифицирующих пользователя:

• внешний аутентифицирующий объект, не принадлежащий системе;

• внутренний объект, принадлежащий системе, в который переносится информация из внешнего объекта.

Внешние объекты могут быть представлены на различных носителях информации — пластиковых картах, смарт-картах, гибких магнитных дисках и т.п. Внешняя и внутренняя формы представления аутентифицирующего объекта должны быть семантически тождественны.

Допустим, что в компьютерной системе зарегистрировано *n* пользователей. Пусть *i-*й аутентифицирующий объект *i*-го пользователя содержит два информационных поля:

*IDi* — неизменный идентификатор i-го пользователя, который является аналогом имени и используется для идентификации пользователя;

*Кi* — аутентифицирующая информация пользователя, которая может изменяться и используется для аутентификации (например, пароль *Рi = Кi )*.

Описанная структура соответствует практически любому Ключевому носителю информации, используемому для опознания пользователя. Например, для носителей типа пластиковых карт выделяются неизменяемая информация *IDi*, первичной персонализации пользователя и объект в файловой структуре Карты, содержащий *Кi*.

Совокупную информацию в ключевом носителе можно назвать первичной аутентифицирующей информацией *i*-го пользователя. Очевидно, что внутренний аутентифицирующий объект не должен существовать в системе длительное время (больше времени работы конкретного пользователя). Для длительного хранения следует использовать данные в защищенной форме.

Системы простой аутентификации на основе многоразовых паролей имеют пониженную стойкость, поскольку в них выбор аутентифицирующей информации происходит из относительно небольшого множества осмысленных слов.

**2. Аутентификация на основе одноразовых паролей**

Более надежными являются процедуры аутентификации на основе одноразовых паролей. Суть схемы одноразовых паролей

— использование различных паролей при каждом новом запросе на предоставление доступа. Одноразовый динамический пароль действителен только для одного входа в систему, и затем его действие прекращается. даже если кто-то перехватил его, пароль окажется бесполезен. динамический механизм выбора пароля — один из лучших способов защиты от угроз перехвата паролей.

Различают следующие способы реализации принципа одноразовых паролей:

• механизм временных меток на основе системы единого времени;

• общий для пользователя и проверяющего список случайных паролей и надежный механизм их синхронизации;

• общий генератор случайных чисел с одним и тем же начальным значением для пользователя и проверяющего.

В основе аутентификации с одноразовыми паролями лежит процедура типа «запрос-ответ». Генерация одноразовых паролей может осуществляться аппаратным или программным способом. Аппаратные средства аутентификации на основе одноразовых паролей часто реализуются в виде миниатюрных устройств со встроенным микропроцессором. Внешне эти устройства похожи на платежные пластиковые карточки. Такие карты обычно называют ключами, У них могут быть клавиатура и небольшое дисплейное окно. Широко известна аппаратная реализация технологии одноразовых паролей SecurID компании Security Dynamics. Существуют и программные реализации средств аутентификации на основе одноразовых паролей в виде программных ключей, в частности продукт Softoken компании Enigma Logic. Программные ключи размещаются на гибком магнитном диске в виде обычной программы с программным генератором одноразовых паролей.

При попытке логического входа в систему пользователь сообщает системе свой идентификатор и затем вводит последовательность цифр, которую сообщает ему аппаратный или программный ключ со встроенным генератором одноразовых паролей. Ключ циклически генерирует новый пароль в виде новой последовательности цифр через небольшие постоянные интервалы времени. Сервер аутентификации сравнивает введенную пользователем цифровую последовательность с выработанным собственным значением и в зависимости от результата этого сравнения разрешает или не разрешает пользователю осуществить логический вход в систему. В качестве сервера аутентификации могут быть использованы выделенный компьютер или программа, выполняемая на обычном сервере.

На практике получила также широкое распространение схема аутентификации на основе одноразовых паролей, предложенная Лампортом. Суть данного метода заключается в многократном использовании партнерами по аутентификационному обмену односторонней функции для генерации разделяемой последовательности одноразовых паролей.

**3. Аутентификация, на основе сертификатов**

Когда число пользователей в сети измеряется миллионами, процедура предварительной регистрации пользователей, связанная с назначением и хранением паролей пользователей, становится крайне громоздкой и практически плохо реализуемой. В таких условиях аутентификация на основе цифровых сертификатов служит рациональной альтернативой применению паролей.

При использовании цифровых сертификатов компьютерная сеть, которая дает доступ к своим ресурсам, не хранит никакой информации о своих пользователях. Эту информацию пользователи предоставляют сами в своих запросах — сертификатах. Такое решение масштабируется гораздо легче, чем вариант с использованием паролей централизованной базой данных. При этом задача хранения секретной информации, в частности закрытых ключей, возлагается теперь на самих пользователей. Цифровые сертификаты, удостоверяющие личность пользователя, выдаются по запросам пользователей специальными уполномоченными организациями — центрами сертификации СА — при выполнении определенных условий. Процедура получения сертификата также включает этап проверки подлинности (то есть аутентификации) пользователя. Здесь в качестве проверяющей стороны выступает сертифицирующая организация.

Для получения сертификата клиент должен представить в центр сертификации СА сведения, удостоверяющие его личность, и свой открытый ключ. Перечень необходимых данных зависит от типа получаемого сертификата. Сертифицирующая организация после проверки доказательств подлинности пользователя помещает свою цифровую подпись в файл, содержащий открытый ключ и сведения о пользователе, и выдает ему сертификат, подтверждая факт принадлежности данного открытого ключа конкретному лицу.

Сертификат представляет собой электронную форму, в которой содержится следующая информация:

• открытый ключ владельца данного сертификата;

• сведения о владельце сертификата, например имя, электронный адрес, наименование организации, в которой работает данный сотрудник и т.п.;

• наименование сертифицирующей организации, выдавшей этот сертификат;

• электронная подпись сертифицирующей организации — зашифрованные закрытым ключом этой организации данные, содержащиеся в сертификате.

Сертификат является средством аутентификации пользователя при его обращении к сетевым ресурсам. При этом роль проверяющей стороны играют серверы аутентификации корпоративной сети. Сертификаты можно использовать не только для аутентификации, но и для предоставления определенных прав доступа. Для этого в сертификат вводятся дополнительные поля, в которых указывается принадлежность его владельца к той или иной категории пользователей.

Следует отметить тесную связь открытых ключей с сертификатами. Сертификат является не только удостоверением личности, но и удостоверением принадлежности открытого ключа. Цифровой сертификат устанавливает и гарантирует соответствие между открытым ключом и его владельцем. Это предотвращает угрозу подмены открытого ключа.

Если абонент получает от партнера по информационному обмену открытый ключ в составе сертификата, то он может проверить цифровую Подпись СА на этом сертификате с помощью открытого ключа данного СА и убедиться, что полученный открытый ключ принадлежит именно тому пользователю, адрес и другие сведения о котором содержатся в данном сертификате. При использовании сертификатов исчезает необходимость хранить на серверах корпораций списки пользователей с их паролями. На сервере достаточно иметь список имен и открытых ключей сертифицирующих организаций.

**Лекция 7**

**БИОМЕТРИЧЕСКАЯ ИДЕНТИФИКАЦИЯ**

**И АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ.**

**СТРОГАЯ АУТЕНТИФИКАЦИЯ**

**1. Биометрическая идентификация и аутентификация пользователей**

Процедуры идентификации и аутентификации пользователя могут базироваться не только на секретной информации, которой обладает пользователь (пароль, секретный ключ, персональный идентификатор и т.п.).

В последнее время все большее распространение получает биометрическая идентификация и аутентификация, позволяющая уверенно идентифицировать потенциального пользователя путем измерения физиологических параметров и характеристик человека, особенностей его поведения.

Основные достоинства биометрических методов идентификации и аутентификации по сравнению с традиционными:

• высокая степень достоверности идентификации по биометрическим признакам из-за их уникальности;

• неотделимость биометрических признаков от дееспособной личности;

• трудность фальсификации биометрических признаков.

В качестве биометрических признаков, которые могут быть использованы при идентификации потенциального пользователя, можно выделить следующие:

• узор радужной оболочки и сетчатки глаз;

отпечатки пальцев;

геометрическая форма руки;

• форма и размеры лица;

• особенности голоса;

• биомеханические характеристики рукописной подписи;.

• биомеханические характеристики <клавиатурного почерка».

При регистрации пользователь должен продемонстрировать один или несколько раз свои характерные биометрические признаки. Эти признаки (известные как подлинные) регистрируются системой в качестве контрольного «образа» законного пользователя. Такой «образ» хранится в электронной форме и используется для проверки идентичности каждого, кто выдает себя за соответствующего законного пользователя. В зависимости от совпадения или несовпадения совокупности предъявленных признаков с зарегистрированными в Контрольном «образе» их предъявивший признается легальным пользователем (при совпадении) или нелегальным (при несовпадении).

Системы идентификации по узору радужной оболочки и сетчатки глаз могут быть разделены на два Класса:

• использующие рисунок радужной оболочки глаза;

• использующие рисунок кровеносных сосудов сетчатки глаза.

Поскольку вероятность повторения данных параметров равна , подобные системы являются наиболее надежными среди всех биометрических систем. Такие средства идентификации применяются там, где требуется высокий уровень безопасности.

Системы идентификации по отпечаткам пальцев — самые популярные. Одной из основных причин их широкого распространения послужило наличие больших банков данных по отпечаткам пальцев. Основными пользователями подобных систем во всем мире являются полиция, различные государственные и некоторые банковские организации.

Системы идентификации по геометрической форме руки используют сканеры формы руки, обычно устанавливаемые на стенах.

Системы идентификации по лицу и голосу наиболее доступны из-за их дешевизны, поскольку большая часть современных компьютеров оснащена видео- и аудиосредствами системы данного класса широко применяются при удаленной идентификации субъекта доступа в телекоммуникационных сетях.

Системы идентификации личностей по динамике рукописной подписи учитывают интенсивность каждого усилия подписывающего, частотные характеристики написания каждого элемента подписи и ее начертание в целом. Системы идентификации по биомеханическим характеристикам «клавиатурного почерка» основываются на том, что моменты нажатия и отпускания клавиш при наборе текста на клавиатуре существенно отличаются у разных пользователей. Динамический ритм набора («клавиатурный почерк») позволяет построить достаточно надежные средства идентификации. В случае обнаружения изменения «клавиатурного почерка» пользователя ему автоматически запрещается работа на ЭВМ.

Применение биометрических параметров при идентификации субъектов доступа автоматизированных систем пока не получило надлежащего нормативно-правового обеспечения, в частности в виде стандартов. Поэтому применение систем биометрической идентификации допускается только в автоматизированных системах, обрабатывающих и хранящих персональные данные, составляющие коммерческую и служебную тайну.

**2. Строгая аутентификация**

Идея строгой аутентификации, реализуемая в криптографических протоколах, заключается в следующем. Проверяемая (доказывающая) сторона доказывает свою подлинность проверяющей стороне, демонстрируя знание какого-либо секрета, который, например, может быть предварительно распределен безопасным способом между сторонами аутентификационного обмена. Доказательство знания секрета осуществляется с помощью последовательности запросов и ответов с использованием криптографических методов и средств.

Существенным является тот факт, что доказывающая сторона демонстрирует только знание секрета, но сам он в ходе аутентификационного обмена не раскрывается. Это обеспечивается посредством ответов доказывающей стороны на различные запросы проверяющей стороны. При этом результирующий запрос зависит только от пользовательского секрета и начального запроса, который обычно представляет произвольно выбранное в начале протокола большое число. В большинстве случаев строгая аутентификация заключается в том, что каждый пользователь аутентифицируется по признаку владения своим секретным ключом, те. пользователь имеет возможность определить, владеет ли его партнер по связи надлежащим секретным ключом и может ли использовать этот ключ для подтверждения того, что действительно является подлинным партнером по информационному обмену.

В соответствии с рекомендациями стандарта Х.509 различают процедуры строгой аутентификации следующих типов:

• односторонняя аутентификация;

• двусторонняя аутентификация;

• трехсторонняя аутентификация.

*Односторонняя аутентификация* предусматривает обмен информацией только в одном направлении.

*Двусторонняя аутентификация* по сравнению с односторонней содержит дополнительный ответ проверяющей стороны доказывающей стороне, который должен убедить ее, что связь устанавливается именно с тем партнером, которому были пред- назначены аутентификационные данные.

*Трехсторонняя аутентификация* содержит дополнительную передачу данных от доказывающей стороны проверяющей. Такой подход позволяет отказаться от использования меток времени при проведении аутентификации.

В зависимости от используемых криптографических алгоритмов протоколы строгой аутентификации можно разделить на следующие группы:

• протоколы строгой аутентификации на основе симметричных алгоритмов шифрования;

• протоколы строгой аутентификации на основе однонаправленных ключевых хэш-функций;

• протоколы строгой аутентификации на основе асимметричных алгоритмов шифрования;

• протоколы строгой аутентификации на основе алгоритмов электронной цифровой подписи.

**2.1. Протоколы аутентификации с симметричными алгоритмами шифрования**

Широко известными представителями протоколов, обеспечивающих аутентификацию пользователей с привлечением в процессе аутентификации третьей стороны, являются протокол распределения секретных ключей Нидхэма и Шредера и протокол Kerberos.

Рассмотрим следующие варианты аутентификации:

• односторонняя аутентификация с использованием меток времени;

• односторонняя аутентификация с использованием случайных чисел;

• двусторонняя аутентификация.

В каждом из этих случаев пользователь доказывает свою подлинность, демонстрируя знание секретного ключа, так как производит с его помощью расшифрование запросов.

Введем следующие обозначения:

— случайное число, сгенерированное участником *А*;

— случайное число, сгенерированное участником *В*;

— метка времени, сгенерированная участником *А*;

— симметричное шифрование на ключе *К* (ключ *К* должен быть предварительно распределен между *А* и *В*).

1. Односторонняя аутентификация, основанная на метках времени:



После получения и расшифрования данного сообщения участник *В* убеждается в том, что метка времени  действительна и идентификатор *В*, указанный в сообщении, совпадает с его собственным. Предотвращение повторной передачи данного сообщения основывается на том, что без знания ключа невозможно изменить метку  идентификатор *В*.

2. Односторонняя аутентификация, основанная на использовании случайных чисел:





Участник *В* отправляет участнику *А* случайное число . Участник *А* шифрует сообщение, состоящее из полученного числа  и идентификатора *В*, и отправляет зашифрованный текст участнику *В*. Последний расшифровывает полученное сообщение и сравнивает содержащееся в нем случайное число с тем, которое он послал участнику *А*. дополнительно он проверяет имя, указанное в сообщении.

3. Двусторонняя аутентификация, использующая случайные значения:



При получении второго сообщения участник *В* выполняет те же проверки, что и в предыдущем протоколе, и дополнительно расшифровывает случайное число  для включения его в третье сообщение для участника *А*.

Третье сообщение, полученное участником *А*, позволяет ему убедиться на основе проверки значений , имеет дело именно с участником *В*.

**2.2. Протоколы, основанные на использовании однонаправленных ключевых хэш-функций**

Своеобразие шифрования с помощью односторонней хэш-функции заключается в том, что оно, по существу, является односторонним, то есть не сопровождается обратным преобразованием — расшифрованием на приемной стороне. Обе стороны (отправитель и получатель) используют одну и ту же процедуру одностороннего шифрования.

Односторонняя хэш-функция (.) С параметром-ключом *К*, примененная к шифруемым данным М, дает в результате хэш-значение *m* (дайджест), состоящее из фиксированного небольшого числа байтов. Дайджест *m =*  *(М)* передается получателю вместе с исходным сообщением *М*. Получатель сообщения, зная, какая односторонняя хэш-функция была применена для получения дайджеста, заново вычисляет ее, используя расшифрованное сообщение *М*. Если значения полученного дайджеста *m* и вычисленного дайджеста *m’* совпадают, значит, содержимое сообщения *М* не было подвергнуто никаким изменениям.

Знание дайджеста не дает возможности восстановить исходное сообщение, но позволяет проверить целостность данных. Дайджест можно рассматривать как своего рода контрольную сумму для исходного сообщения. Однако между дайджестом и обычной контрольной суммой имеется и существенное различие. Контрольную сумму используют как средство про верки целостности передаваемых сообщений по ненадежным линиям связи. Это средство проверки не рассчитано на борьбу со злоумышленниками, которым в такой ситуации ничто не мешает подменить сообщение, добавив к нему новое значение контрольной суммы. Получатель в таком случае не заметит никакой подмены.

В отличие от обычной контрольной суммы, при вычислении дайджеста применяются секретные ключи. В случае если для получения дайджеста используется односторонняя хэш-функция с параметром-ключом *К*, который известен только отправителю и получателю, любая модификация исходного сообщения будет немедленно обнаружена.

Существует другой вариант использования односторонней хэш-функции для проверки целостности данных. В этом случае односторонняя хэш-функция *h(.)* не имеет параметра-ключа, но зато применяется не просто к сообщению *М*, а к сообщению, дополненному секретным ключом *К*, то есть отправитель вычисляет дайджест *m= h(М, К)*. Получатель, извлекая исходное сообщение *М*, также дополняет его тем же известным ему секретным ключом *К*, после чего применяет к полученным данным одностороннюю хэш-функцию *h(.)*. Результат вычислений — дайджест *m’* — сравнивается с полученным по сети дайджестом *m*.