Мерзлякова Е.Ю.

АУТЕНТИФИКАЦИЯ И УПРАВЛЕНИЕ ДОСТУПОМ

Элементы аутентификации

- **Аутентификация** (от греч. — истинный, реальный) — установление (подтверждение) подлинности субъекта или его права доступа к информационным ресурсам веб-сайта или системы согласно предъявленному им идентификатором. Процесс аутентификации состоит из определенного набора элементов:
- субъекта, проходящего аутентификацию (авторизированного пользователя);
- характеристики субъекта (идентификатора, предъявляемого им для проверки подлинности);
- владельца системы аутентификации (хозяина веб-сайта или информационного ресурса);
- механизма аутентификации (ПО, проверяющего подлинность предъявленного идентификатора);
- механизма авторизации (предоставления или лишения субъекта прав доступа в зависимости от успешной или безуспешной процедуры аутентификации).

Типы аутентификации

- *уникальная последовательность символов*, которую пользователь должен знать для успешного прохождения аутентификации. Простейший пример - парольная аутентификация, для которой достаточно ввести в систему свой идентификатор (например, логин) и пароль.

- *уникальное содержимое* или *уникальные характеристики* предмета. В этом качестве выступают любые внешние носители информации: смарт-карты, мобильные телефоны и т.д.

- по *биометрической информации*, которая неотъемлема от пользователя

Удаленная аутентификация. Доступ по паролю

- Вся информация о пользователе (логин и пароль) передается по сети в открытом виде. Полученный сервером пароль сравнивается с эталонным паролем данного пользователя, который хранится на сервере. В целях безопасности на сервере чаще хранятся не пароли в открытом виде, а их хэш-значения.
- 

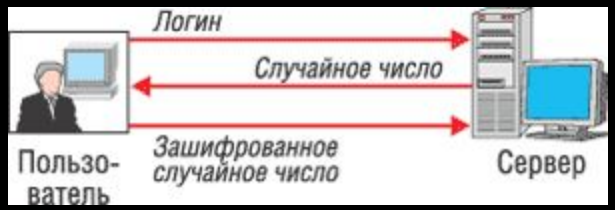
(Password Access Protocol, PAP)
- недостатки: любой злоумышленник, способный перехватывать сетевые пакеты, может получить пароль пользователя с помощью простейшего анализатора пакетов. Любой потенциальный пользователь системы должен предварительно зарегистрироваться в ней

Удаленная аутентификация. Запрос-ответ

- пользователь посылает серверу запрос на доступ, включающий его логин;
- сервер генерирует случайное число и отправляет его пользователю;
- пользователь шифрует полученное случайное число симметричным алгоритмом шифрования на своем уникальном ключе и результат зашифрования отправляется серверу;
- сервер расшифровывает полученную информацию на том же ключе и сравнивает с исходным случайным числом. При совпадении чисел пользователь считается успешно аутентифицированным, поскольку признается владельцем уникального секретного ключа.

Удаленная аутентификация. Запрос-ответ

- Аутентифицирующей информацией в данном случае служит ***ключ***, на котором выполняется шифрование случайного числа. Он никогда не передается по сети, а лишь участвует в вычислениях, что составляет несомненное преимущество протоколов данного семейства.

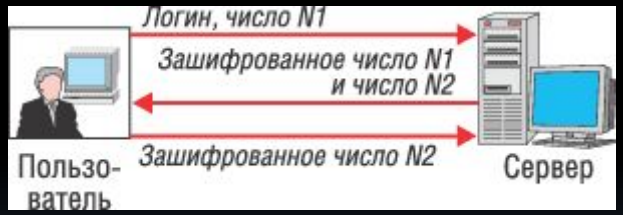


- CHAP (Challenge-Handshake Authentication Protocol)

- Недостаток: необходимость иметь на локальном компьютере клиентский модуль, выполняющий шифрование.
- Однако в качестве клиентского компьютера может выступать "носимое" устройство, обладающее достаточной вычислительной мощностью, например, мобильный телефон. В таком случае теоретически допустима аутентификация и получение доступа к серверу с любого компьютера, оснащенного устройством чтения смарт-карт, с мобильного телефона или КПК.

Удаленная аутентификация. Запрос-ответ

- Протоколы типа "запрос-ответ" легко "расширяются" до схемы взаимной аутентификации :
- *пользователь посылает свое случайное число (N1).*
- *сервер, помимо своего случайного числа (N2), должен отправить еще и число N1, зашифрованное соответствующим ключом.*
- *пользователь расшифровывает полученный N1 и проверяет: совпадение расшифрованного числа с его N1 указывает, что это именно тот сервер, который нужен пользователю.*
- Такая процедура аутентификации часто называется ***рукопожатием***.



- Аутентификация будет успешна только в том случае, если пользователь предварительно зарегистрировался на данном сервере и каким-либо образом обменялся с ним секретным ключом.
- Вместо симметричного шифрования в протоколах данного семейства может применяться и асимметричное шифрование, и электронная цифровая подпись. В таких случаях схему аутентификации легко расширить на неограниченное число пользователей.

Протокол Kerberos

Протокол Kerberos

- При использовании Kerberos нельзя напрямую получить доступ к какому-либо целевому серверу;
- чтобы запустить процедуру аутентификации, необходимо обратиться к специальному серверу аутентификации с запросом, содержащим логин пользователя;
- если сервер не находит автора запроса в своей базе данных, запрос отклоняется;
- в противном случае сервер аутентификации формирует случайный ключ, который будет использоваться для шифрования сеансов связи пользователя с еще одним специальным сервером системы: сервером предоставления билетов (Ticket-Granting Server, TGS);
- данный случайный ключ (обозначим его Ku-tgs) сервер аутентификации зашифровывает на ключе пользователя (Kuser) и отправляет последнему;

Протокол Kerberos

- Дополнительная копия ключа Ku-tgs с рядом дополнительных параметров (называемая билетом) также отправляется пользователю зашифрованной на специальном ключе для связи серверов аутентификации и TGS (Ktgs);
- пользователь не может расшифровать билет, который необходим для передачи серверу TGS на следующем шаге аутентификации;
- следующее действие пользователя - запрос к TGS, содержащий логин пользователя, имя сервера, к которому требуется получить доступ, и тот самый билет для TGS;
- в запросе всегда присутствует метка текущего времени, зашифрованная на ключе Ku-tgs для предотвращения атак, выполняемых повтором перехваченных предыдущих запросов к серверу. Поэтому системное время всех компьютеров, участвующих в аутентификации по протоколу Kerberos, должно быть строго синхронизировано.

Протокол Kerberos

- в случае успешной проверки билета сервер TGS генерирует еще один случайный ключ для шифрования сеансов связи между пользователем, желающим получить доступ, и целевым сервером (Ku-serv);
- этот ключ шифруется на ключе Kuser и отправляется пользователю;
- копия ключа Ku-serv и необходимые целевому серверу параметры аутентификации (билет для доступа к целевому серверу) посылаются пользователю еще и в зашифрованном виде (на ключе для связи TGS и целевого сервера - Kserv);
- теперь пользователь должен послать целевому серверу полученный на предыдущем шаге билет, а также метку времени, зашифрованную на ключе Ku-serv;

Протокол Kerberos

- после успешной проверки билета пользователь наконец-то считается аутентифицированным и может обмениваться информацией с целевым сервером;
- ключ Ku-serv, уникальный для данного сеанса связи, часто применяется и для шифрования пересылаемых в этом сеансе данных;
- если пользователю необходим доступ к нескольким серверам, он снова формирует запросы к серверу TGS - столько раз, сколько серверов нужно ему для работы. Сервер TGS генерирует для каждого из таких запросов новый случайный ключ Ku-serv, т. е. все сессии связи с различными целевыми серверами защищены при помощи разных ключей.

Протокол Kerberos. Недостатки

- необходимость установки достаточно сложного клиентского ПО;
- необходимость в нескольких специальных серверах (доступ к целевому серверу обеспечивают как минимум еще два, сервер аутентификации и TGS);
- теоретически злоумышленник, получивший доступ к TGS или серверу аутентификации, способен вмешаться в процесс генерации случайных ключей или получить ключи всех пользователей и, следовательно, инициировать сеансы связи с любым целевым сервером от имени любого легального пользователя.

Биометрические технологии

Регистрация идентификатора — сведения о физиологической или поведенческой характеристике преобразуются в форму, доступную компьютерным технологиям, и вносятся в память биометрической системы;

Выделение признаков — из вновь предъявленного идентификатора выделяются уникальные признаки, анализируемые системой;

Сравнение — сопоставляются сведения о вновь предъявленном и ранее зарегистрированном идентификаторе;

Решение — вносится заключение о том, совпадают или не совпадают вновь предъявленный и ранее зарегистрированный идентификатор.

Биометрические технологии.

Статические методы идентификации

- основаны на анализе неизменных физиологических характеристик человека
- наиболее распространены

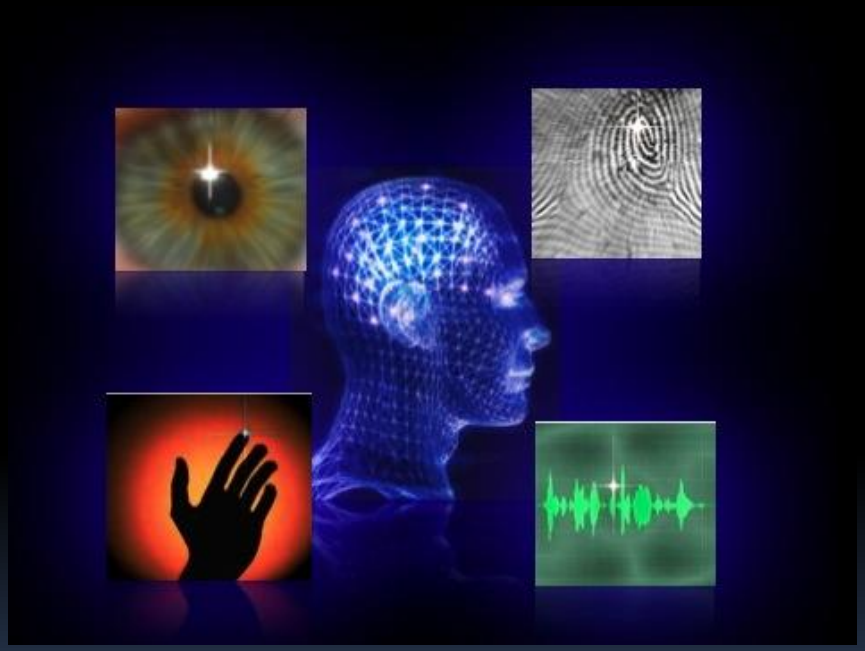
Динамические методы идентификации

- основываются на анализе поведенческих характеристик личности — особенностей, присущих каждому человеку в процессе воспроизведения какого-либо действия.
- динамические методы существенно уступают статическим в точности и эффективности и, как правило, используются в качестве вспомогательных.

Биометрические технологии

Статические идентификаторы

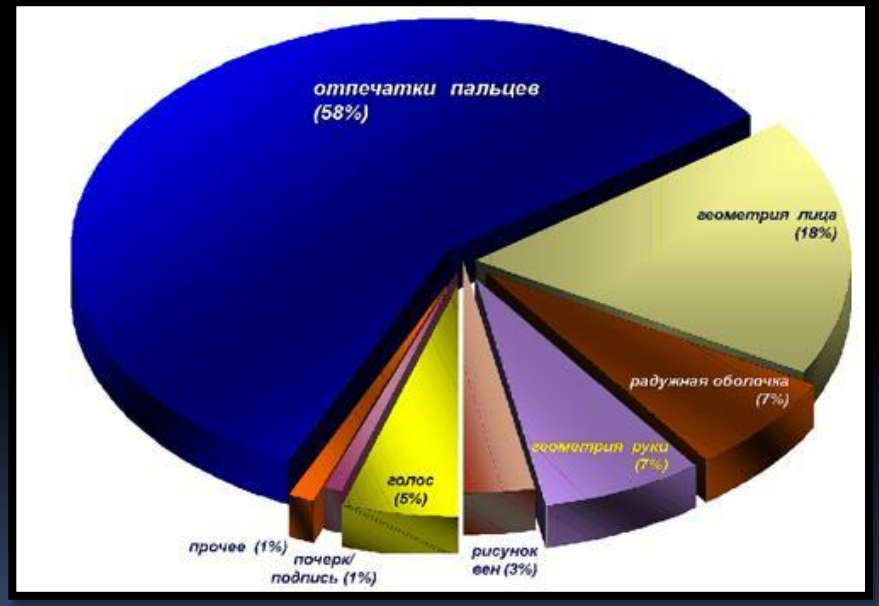
- ***отпечатки пальцев (***на использовании этих идентификаторов строится самая распространенная, удобная и эффективная биометрическая технология);
- ***форма и геометрия лица*** (с этими идентификаторами работают технологии распознавания двумерных изображений лиц, черпаемых из фотографий и видеоряда);
- ***форма и строение черепа*** (для большей благозвучности компании, действующие в данной сфере, предпочитают говорить о технологиях распознавания человека по трехмерной модели лица);
- ***сетчатка глаза, радужная оболочка*** (практически не используется в качестве идентификатора);
- ***геометрия ладони, кисти руки или пальца*** (используется в нескольких узких сегментах рынка);
- ***рисунок вен на ладони или пальце руки*** (соответствующая технология становится популярной, но ввиду дороговизны сканеров пока не используется широко);
- ***ДНК*** (в основном в сфере специализированных экспертиз);



Биометрические технологии

Динамические идентификаторы

- динамика подписи;
- динамика клавиатурного набора;
- голос;
- движение губ;
- походка;
- особенности начертания рукописного текста.



Биометрические технологии

Режим идентификации

- Сравнение идет в режиме «один-ко-многим» (1: N): вновь предъявленный идентификатор сравнивается со всеми ранее зарегистрированными.
- биометрическая система ищет ответ на вопрос «Кто Вы?»,

Режим верификации

- Сравниваются сведения о двух конкретных идентификаторах (режим «один-к-одному», или 1:1).
- формируется ответ на вопрос «Вы действительно тот, за кого себя выдаете?».

Биометрические технологии

Правоохранительная деятельность

- Обязательная регистрация;
- Используются отпечатки пальцев (как правило, всех десяти) и ладоней, фотографии;
- Идентификаторы получают с помощью отпечатков на бумаге, стекле и т.п. поверхностях;
- Возможно извлечь идентификатор из базы данных;
- Необходимо привлечение высококвалифицированных специалистов;
- Области применения ограничены и включают регистрацию представителей отдельных слоев общества в целях борьбы с преступностью, терроризмом, нелегальной миграцией.

Гражданская идентификация

- Добровольная регистрация;
- Используются отпечатки пальцев (1-2, редко более), радужная оболочка, лицо, рисунок вен, геометрия кисти руки и др.;
- Идентификаторы получают исключительно путем электронного сканирования;
- Восстановить идентификатор из его модели невозможно;
- Достаточно базовых навыков работы с компьютером;
- Области применения разнообразны и охватывают идентификацию избирателей, пользователей услуг предприятий транспортной, финансовой, социальной, медицинской, культурной, спортивной, досуговой и многих других сфер.

Методы и средства защиты от удаленных атак

Межсетевой экран – это система межсетевой защиты, позволяющая разделить общую сеть на две части или более и реализовать набор правил, определяющих условия прохождения пакетов с данными через границу из одной части сети в другую.

МЭ пропускает через себя весь трафик, принимая для каждого проходящего пакета решение – пропустить его или отбросить.

Основные компоненты МЭ –это

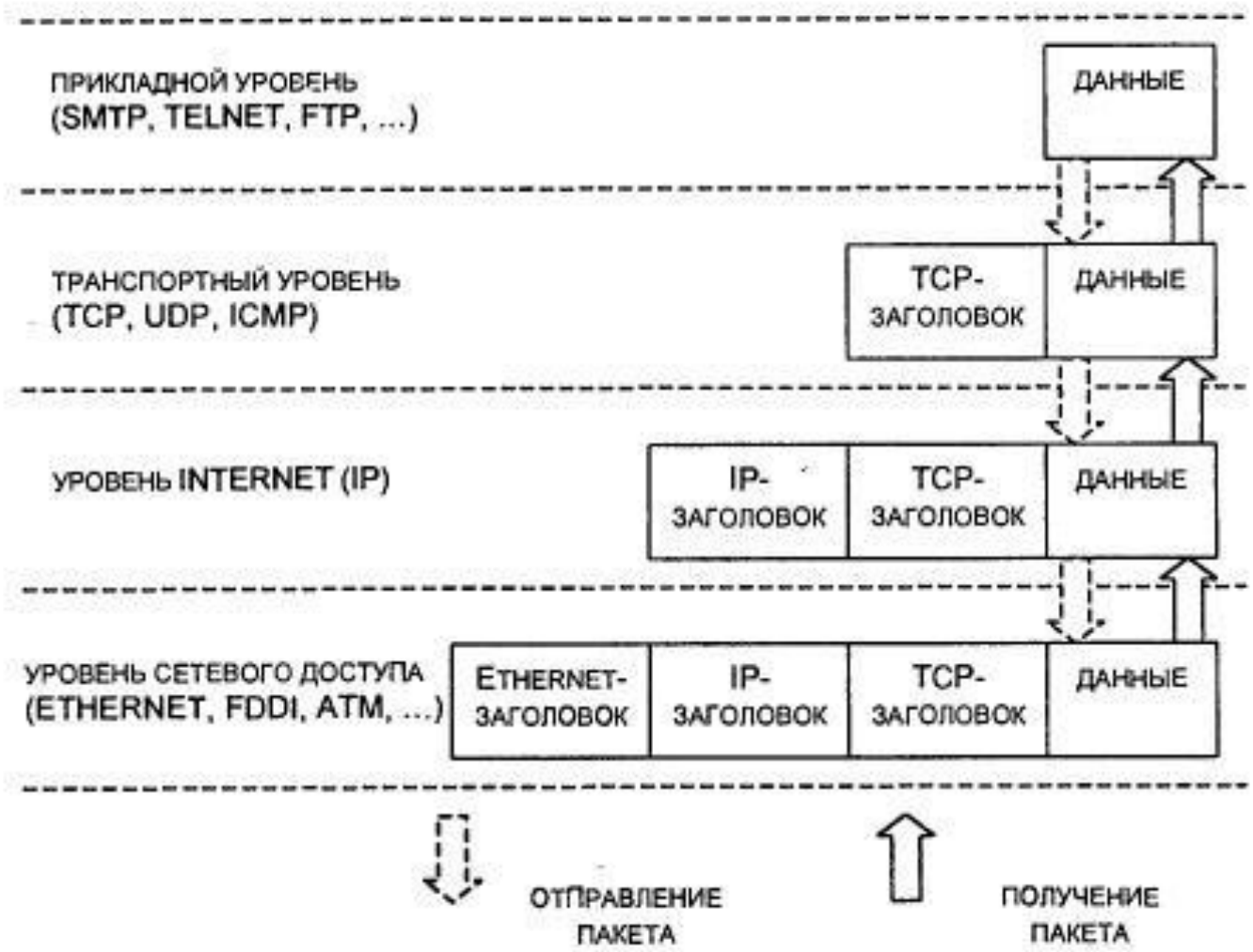
- Фильтрующие маршрутизаторы
- Шлюзы сетевого уровня
- Шлюзы прикладного уровня

Фильтрующие маршрутизаторы

- ФМ – это маршрутизатор или работающая на сервере программа, сконфигурированные так, чтобы фильтровать входящие и исходящие пакеты;

- Фильтрация пакетов осуществляется на основе информации, содержащийся в TCP- и IP- заголовках пакетов.

Фильтрующие



Фильтрующие маршрутизаторы

Фильтрация IP-пакетов происходит на основе группы полей заголовка пакета:

- IP-адрес отправителя (адрес системы, которая послала пакет);
- IP-адрес получателя (адрес системы, которая принимает пакет);
- Порт отправителя;
- Порт получателя;

Порт – это программное понятие, которое используется клиентом или сервером для посылки или приема сообщений.

Пример работы ФМ

Задача: ***реализовать политику безопасности, допускающую определенные соединения с внутренней сетью с адресом 123.4.*.****

- Соединения TELNET только с одним хост-компьютером с адресом 123.4.5.6
- Соединения SMPT только с двумя хост-хост компьютерами 123.4.5.7 и 123.4.5.8
- Обмен по NNTP (Network News Transfer Protocol) только от сервера новостей с адресом 129.6.48.254 и только с NNTP-сервером сети с адресом 123.4.5.9
- Протокол NTP для всех хост-компьютеров;
- Все другие серверы и пакеты блокируются;

Пример работы ФМ

Правила фильтрации

Тип	Адрес отправителя	Адрес получателя	Порт отправителя	Порт получателя	Действие
TCP	*	123.4.5.6	>1023	23	Разрешить
TCP	*	123.4.5.7	>1023	25	Разрешить
TCP	*	123.4.5.8	>1023	25	Разрешить
TCP	129.6.48.254	123.4.5.9	>1023	119	Разрешить
UDP	*	123.4.*.*	>1023	123	Разрешить
*	*	*	*	*	Запретить

Первое правило позволяет пропускать пакеты TCP из сети Internet от любого источника с номером порта, большим 1023, к получателю с адресом 123.4.5.6. в порт 23. Порт 23 связан с сервером TELNET, а все его клиенты должны иметь порты с номерами не ниже 1024.

Второе и третье правила работают аналогично и разрешают передачу пакетов к получателям с адресами 123.4.5.7 и 123.4.5.8 в порт 25, используемый SMTP.

Четвертое правило пропускает пакеты к NNTP-серверу сети только от конкретного отправителя к конкретному получателю.

Пятое правило разрешает трафик NTP, который использует протокол UDP вместо TCP, от любого источника к любому получателю внутренней сети;

Шестое правило блокирует все остальные пакеты.

Достоинства ФМ

- Сравнительно невысокая стоимость;
- Гибкость в определении правил фильтрации;
- Небольшая задержка при прохождении пакетов;

Недостатки ФМ

- Правила фильтрации пакетов формируются сложно, автоматизированных средств тестирования их корректности обычно нет;
- Внутренняя сеть видна из сети Internet;
- Отсутствует аутентификация на пользовательском уровне;
- При нарушении работоспособности МЭ все компьютеры за ним становятся незащищены либо недоступны;
- При частом отсутствии средств протоколирования опасные пакеты не смогут быть выявлены до обнаружения последствий;
- Широко распространен и эффективен вид нападения «подмена адреса», когда хакер использует реальный доверенный адрес для своего вредоносного пакета.
- МЭ легко «обмануть», когда проверяется только информация IP-заголовков – хакер создает заголовок, который удовлетворяет правилам, остальная информация не проверяется и может нести вред.

Шлюзы сетевого уровня