Лекция №20

Авторизация и аутоидентификация

Определение

- **Аутентифика́ция** (*Authentication*) — проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.
- Аутентификацию не следует путать с идентификацией.
- Аутентификатор - это пакет, доказывающий, что клиент действительно является обладателем секретного ключа.

Способы аутентификации

- Текстовый ввод логина и пароля
- Электронные сертификаты
- Пластиковые карты
- Биометрические устройства:
  сканеров радужной оболочки
  лаза или отпечатков пальцев или ладони
- Смарт-карты

Протоколы аутентификации

- Процедура аутентификации используется при обмене информацией между компьютерами, при этом используются весьма сложные криптографические протоколы, обеспечивающие защиту линии связи от прослушивания или подмены одного из участников взаимодействия. А поскольку, как правило, аутентификация необходима обоим объектам, устанавливающим сетевое взаимодействие, то аутентификация должна быть взаимной.
- В частности, в операционных системах семейства WindowsNT 4 используется протокол NTLM (NT LAN Manager — Диспетчер локальной сети NT). А в доменах Windows 2000/2003 применяется гораздо более совершенный протокол Kerberos, который предлагает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними, причём в протоколе учтён тот факт, что начальный обмен информацией между клиентом и сервером происходит в незащищённой среде, а передаваемые пакеты могут быть перехвачены и модифицированы. Другими словами, протокол идеально подходит для применения в Интернет и аналогичных сетях.

Базы учетных записей

- Один из способов аутентификации в компьютерной системе состоит во вводе вашего пользовательского идентификатора, в просторечии называемого «логином» (*login* — регистрационное имя пользователя) и пароля — некой конфиденциальной информации, знание которой обеспечивает владение определенным ресурсом. Получив введенный пользователем логин и пароль, компьютер сравнивает их со значением, которое хранится в специальной базе данных и, в случае совпадения, пропускает пользователя в систему.
- На компьютерах с ОС семейства UNIX, базой является файл /etc/master.passwd (в дистрибутивах Linux обычно файл /etc/shadow, доступный для чтения только root), в котором пароли пользователей хранятся в виде хеш функций от открытых паролей, кроме этого в этом же файле хранится информация о правах пользователя. Изначально в Unix — системах пароль (в зашифрованном виде) хранился в файле /etc/passwd, доступном для чтения всем пользователям, что было небезопасно.
- На компьютерах с операционной системой Windows (не входящих в домен Windows) такая база данных называется SAM (Security Accoun Manager — Диспетчер защиты учётных записей). База SAM хранит учётные записи пользователей, включающие в себя все данные, необходимые системе защиты для функционирования. Находится в директории %windir%\system32\config\.
- В доменах Windows Server 2000/2003 такой базой является ActiveDirectory.
- Однако более надёжным способом хранения аутентификационных данных признано использование специальных аппаратных средств (компонентов).
- При необходимости обеспечения работы сотрудников на разных компьютерах (с поддержкой системы безопасности) используют аппаратно-программные системы, позволяющие хранить аутентификационные данные и криптографические ключи на сервере организации. Пользователи свободно могут работать на любом компьютере (рабочей станции), имея доступ к своим аутентификационным данным и криптографическим ключам.

Определение

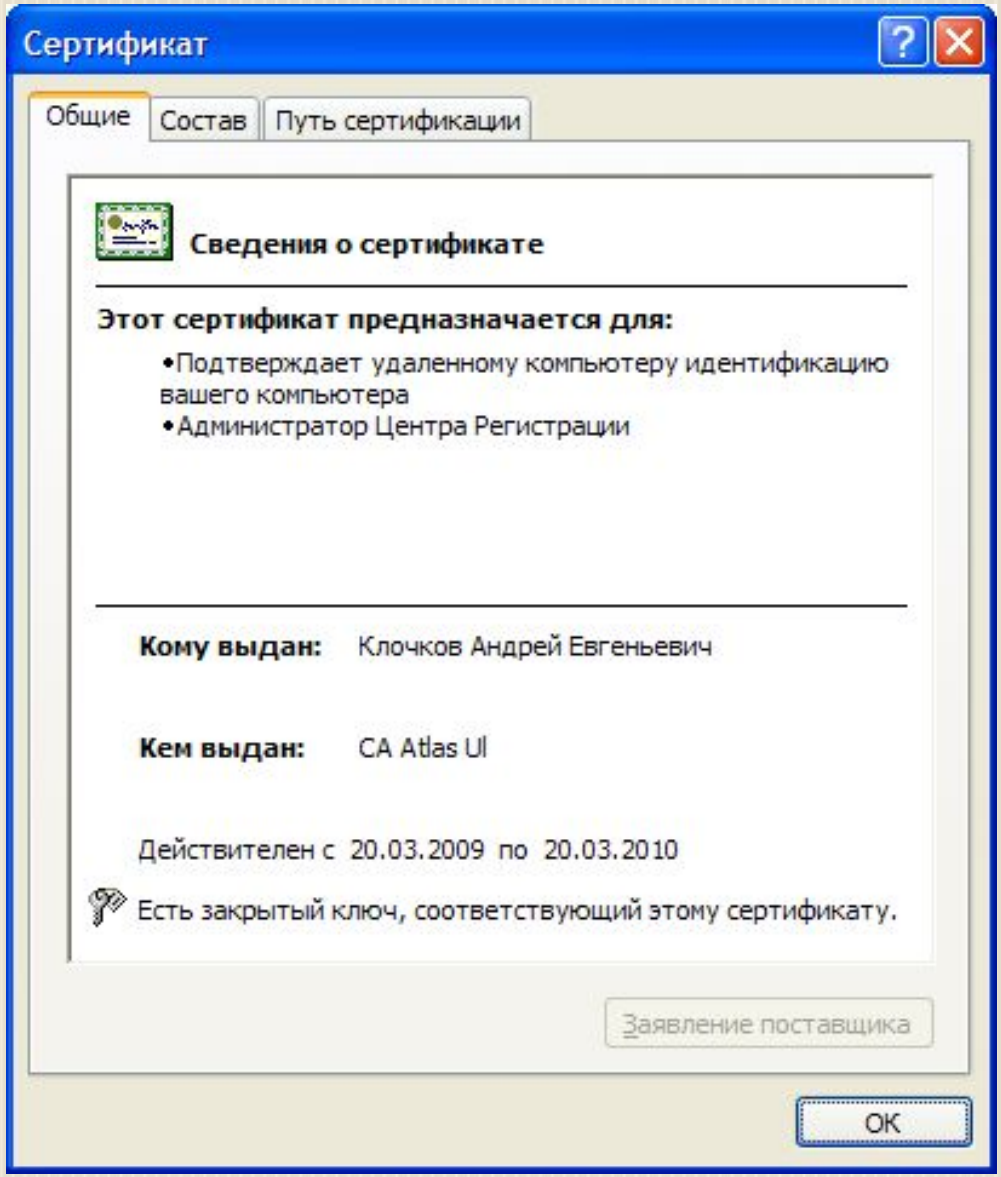
- **Авторизация** (*authorization*):
  - 1. Процесс предоставления определенному лицу прав на выполнение некоторых действий.
  - 2. Процесс подтверждения (проверки) прав пользователей на выполнение некоторых действий

- Авторизацию не следует путать с аутентификацией: аутентификация — это установление подлинности лица, а авторизация — предоставление этому лицу некоторых прав или проверка их наличия (как правило — следующий шаг системы после аутентификации).

Авторизация

- В информационных технологиях посредством авторизации устанавливаются и реализуются права доступа к ресурсам и системам обработки данных.
- Механизмы авторизации в операционных системах:
  - использование полномочий;
  - использование списка контроля доступа (ACL).

Сертификаты



Security Account Manager

- **SAM**— RPC-сервер Windows, оперирующий базой данных учетных записей.
- SAM выполняет следующие задачи:
- Идентификация субъектов (трансляции имен в идентификаторы (SID'ы) и обратно);
- Проверка пароля, авторизация (участвует в процессе входа пользователей в систему);
- Хранит статистику (время последнего входа, количества входов, количества некорректных вводов пароля);
- Хранит настройки политики учетных записей и приводит их в действие (политика паролей и политика блокировки учетной записи);
- Хранит логическую структуру группировки учетных записей (по группам,доменам,алиасам);
- Контролирует доступ к базе учетных записей;
- Предоставляет программный интерфейс для управления базой учетных записей.

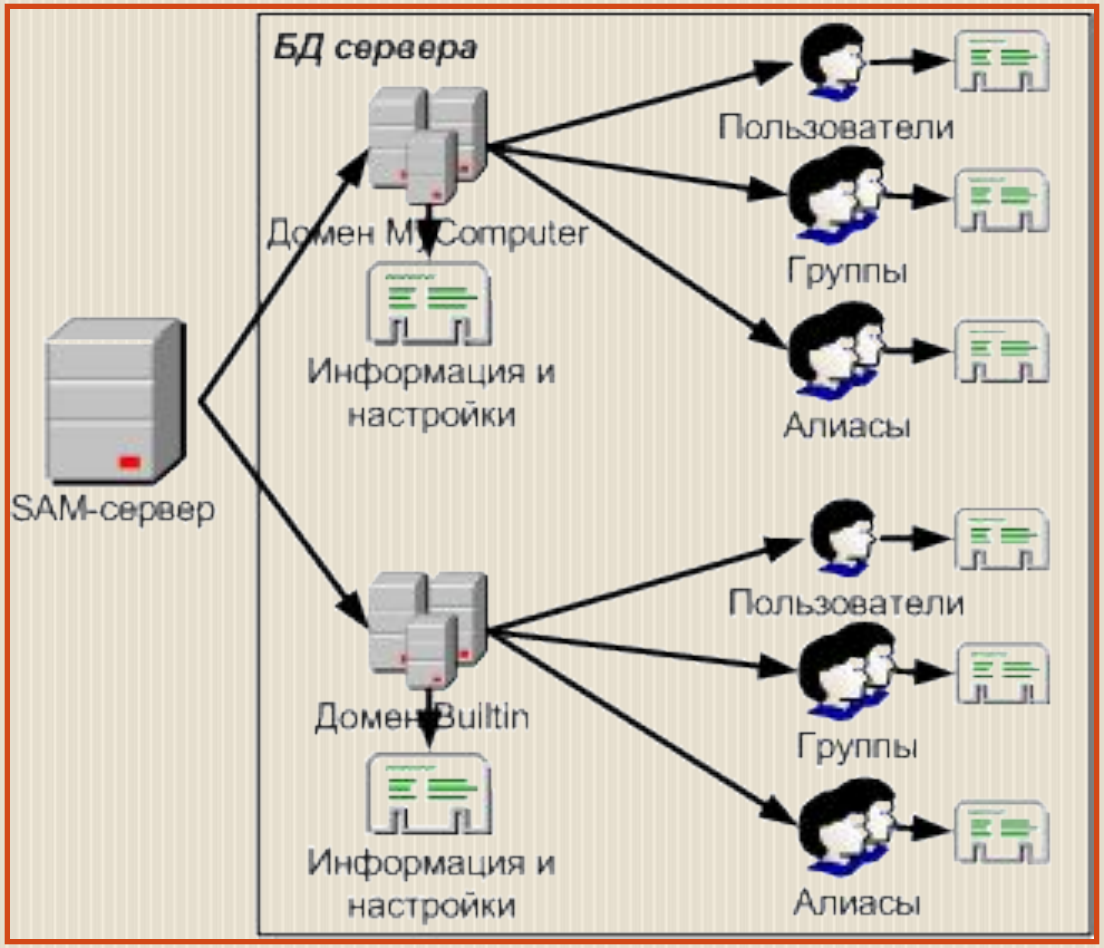
Security Account Manager

- База данных SAM хранится в реестре (в ключе HKEY_LOCAL_MACHINE\SAM\SAM), доступ к которому запрещен по умолчанию даже администраторам.
- SAM-сервер реализован в виде DLL-библиотеки samsrv.dll, загружаемой lsass.exe. Программный интерфейс для доступа клиентов к серверу реализован в виде функций, содержащихся в DLL-библиотеке samlib.dll.

Объекты сервера SAM

- Сервер SAM оперирует с несколькими типами объектов, или сущностей, каждая из которых защищается списком контроля доступа и содержит ряд свойств, которые могут быть изменены. Сервер SAM хранит следующие типы объектов:
- Сервер - хранит список объектов-доменов и позволяет получить доступ к объектам-доменам;
- Домен - хранит учетные записи пользователей, групп, алиасов, позволяет ими управлять, хранит политику учетных записей и позволяет ее изменять;
- Пользователь - учетная запись пользователя компьютера или учетная запись компьютера, хранит идентификатор, свойства, пароль, статистику, комментарии;
- Алиас - учетная запись, позволяющая группировать пользователей, другие алисы и группы. Содержит имя, комментарий и список членов. Алисы в стандартных оснастках управления учетными записями Windows называются группами;
- Группа - учетная запись, позволяющая в отличие от алиса группировать только пользователей. Каждый пользователь должен состоять как минимум в одной группе. В оснастках управления учетными записями эти объекты называются глобальными группами

Объекты сервера SAM



Процесс аутентификации клиент-серверных приложений в сетях Microsoft

- Появляется запрос локальной подсистемы безопасности (Local Security Authority, LSA) на ввод имени пользователя и пароля.
- После ввода пароль хэшируется (криптографический хэш - одностороннее преобразование делающее невозможным, или по крайней мере сложным восстановление по нему оригинального пароля) и хэш помещается в хранилище LSA.
- В хранилище хэши находятся до окончания сеанса работы (а иногда и после, это будет рассмотрено далее).