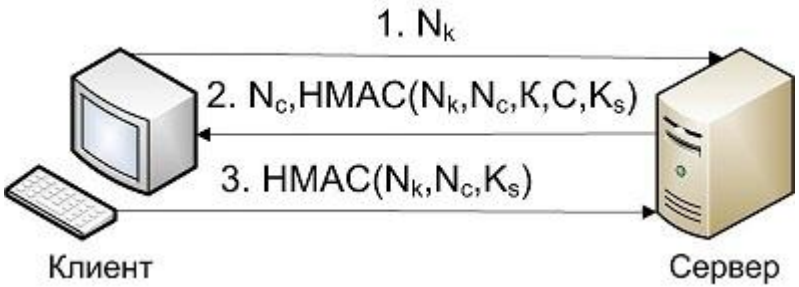
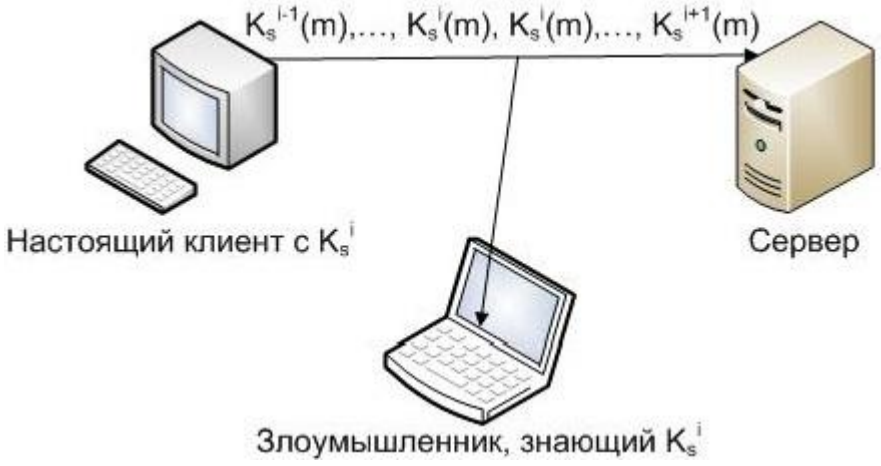
Безопасная аутентификация



Безопасность сети – ключевая проблема, стоящая перед ИТ-службами. Решение формируется из комплекса элементов, один из них – **безопасная аутентификация**

Важным вопросом является **обеспечение процедуры безопасной аутентификации**.

Вопросы безопасной аутентификации являются весьма актуальными при попытке обеспечения безопасности организации в целом.



ИДЕНТИФИКАЦИЯ

-это процедура распознавания субъекта по его идентификатору. В процессе регистрации выполняется предъявление идентификатора системе, и она проверяет его наличие в своей базе данных. Только субъекты с известными системе идентификаторами считаются легальными.

Аутентификация

– процедура проверки подлинности, позволяющая достоверно убедиться в том, что предъявивший свой идентификатор на самом деле является именно тем, за кого он себя выдает. Для этого он должен подтвердить факт обладания некоторой информацией, которая может быть доступна только ему одному (пароль, ключ и т.п.).

Авторизация

– процедура предоставления определенных прав доступа к ресурсам системы после прохождения им процедуры аутентификации. Для каждого субъекта в системе определяется набор прав, которые он может использовать при обращении к ее ресурсам.

Администрирование

- процесс управления доступом к ресурсам системы. Этот процесс включает в себя:
  - создание идентификатора (создание учетной записи пользователя) в системе;
  - управление данными пользователя, применяемыми для его аутентификации (смена пароля, издание сертификата и т.п.);
  - управление правами доступа к ресурсам системы.

Аудит

– процесс контроля доступа к ресурсам системы, включающий протоколирование действий при доступе к ресурсам системы для обеспечения возможности обнаружения попыток несанкционированных действий.

Для подтверждения своей подлинности необходимо предоставить некоторую секретную информацию. Существуют различные виды такой информации, которые можно обозначить одним термином «**фактор аутентификации**».

Фактор аутентификации – определенный вид информации, предоставляемый субъектом системе при его аутентификации. Данная процедура может быть реализована с использованием одного или нескольких аутентификационных факторов. Например, у пользователя может быть запрошен пароль либо потребуется предоставить отпечаток пальца.

Однофакторная аутентификация – процесс, в котором используется только один тип аутентификационных факторов.

Многофакторная аутентификация – процесс, в котором используется несколько факторов. Например, при регистрации пользователь должен использовать смарт-карту и пароль.

Классификация типов факторов аутентификации

На основе знания чего-либо (Authentication by Knowledge):

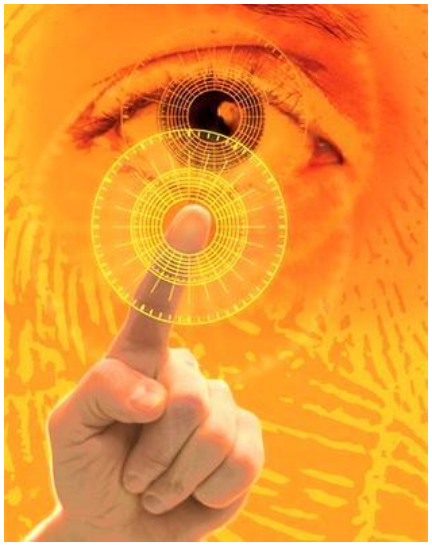
- пароль или парольная фраза;
- PIN.

На основе обладания чем-либо (Authentication by Ownership):

- физический ключ;
- карта с магнитной полосой;
- OTP-токен, генерирующий одноразовый пароль.

На основе биометрии (Authentication by Characteristic):

- отпечаток пальца;
- рисунок сетчатки глаза;
- голос.



В некоторых компаниях организуется строгий контроль доступа в помещение, то есть в определенные помещения доступ предоставляется **только ограниченному числу лиц**.

В этом случае иногда говорят об использовании четвертого типа фактора аутентификации – на **основе места проведения процедуры**, однако это не считается дополнительным типом факторов аутентификации, так как он не может использоваться отдельно от других.

В последнее время наметились тенденции интеграции логических средств аутентификации и средств контроля и управления доступом (СКУД). Смарт-карты, используемые для аутентификации пользователя при попытке доступа к ресурсам компьютерной системы, интегрируются с RFID (радио-частотной идентификацией).

Особенности аутентификации по паролю. Риски парольной аутентификации и методы борьбы с ними

Для пользователей наиболее широко используется **аутентификация по секретной информации, которая неизвестна непосвященным людям**.

Это может быть вводимый с помощью клавиатуры набор символов.

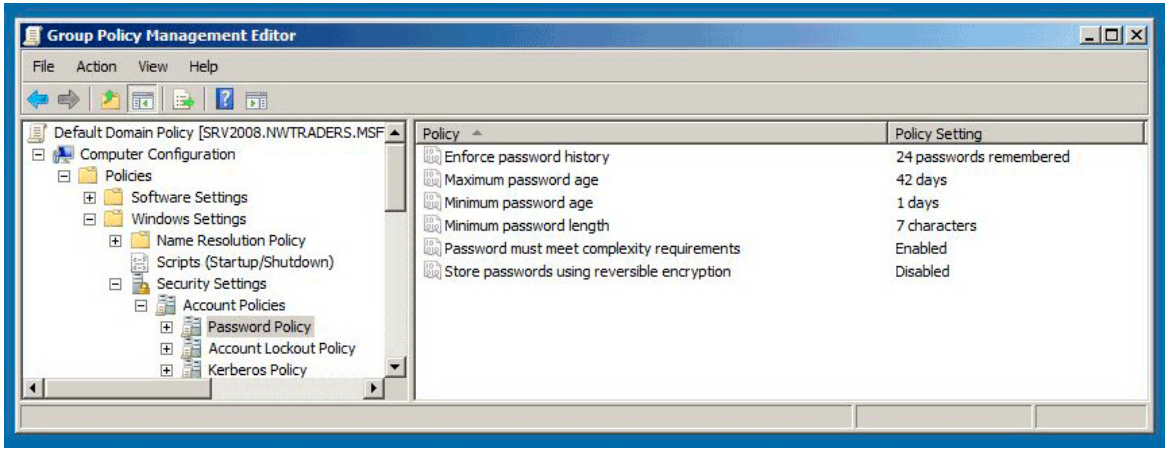
Чем длиннее пароль или идентификационная фраза, тем он более устойчив к взлому (сложнее поддается подбору, перебору или другим типам атак). Хорошим вариантом считается идентификационная фраза длиной от 25 до 100 символов.

Типовые атаки на пароль

- Методы перебора паролей. Атака со словарем
- Социотехника, угадывание, подглядывание
- «Троянский конь»
- Принуждение

Методы защиты при использовании аутентификации по паролю

- Для защиты паролей от взлома следует настроить соответствующую политику в Windows Server 2008.



- задать минимальную длину пароля
- включить требование сложности
- задать его максимальный срок жизни
- настроить хранение истории паролей
- задать минимальный срок, в течение которого пароль нельзя поменять
- настроить блокировку учетной записи при неоднократном неправильном вводе пароля

Для защиты от «троянских коней» следует использовать антивирусные средства и блокировку несанкционированного программного обеспечения.

Для ограничения возможностей пользователей по внесению вирусов в информационную систему оправданы: настройка запрета на работу с внешними устройствами (CD, DVD, Flash), строгий режим работы UAC, использование отдельно стоящих интернет-киосков на базе компьютеров, не входящих в состав рабочей сети

Человеческий фактор – самая большая угроза

Инсайдинг- существенная угроза безопасности заключается в потенциальной возможности физического доступа злоумышленника к рабочей станции легального пользователя и передача конфиденциальной информации третьим лицам.

Двухфакторная аутентификация

- **1-й фактор** – обладание паролем
- **2-й – знание PIN-кода**

Доменный пароль больше не набирается на клавиатуре, значит, не перехватывается клавиатурным шпионом. Перехват доменного пароля чреват возможностью входа, перехват PIN-кода не так опасен, так как дополнительно требуется смарт-карта.

Внедрение двухфакторной аутентификации на основе асимметричной криптографии в AD DS

- Служба каталога Active Directory поддерживает возможность аутентификации с помощью смарт-карт

Возможность аутентификации с помощью смарт-карт заложена в расширении **PKINIT** (public key initialization – инициализация открытого ключа) для протокола **Kerberos** RFC 4556.

Расширение PKINIT позволяет использовать сертификаты открытого ключа на этапе предаутентификации Kerberos.