

TechDays.ru

Двухфакторная аутентификация в Службе Каталога AD DS

Леонид Шапиро
МСТ
ЦКО «Специалист»

компьютерного
Центр
ОБУЧЕНИЯ
«СПЕЦИАЛИСТ»
при МГТУ им. Н.Э.Баумана

Обзор

- Что такое аутентификация
- Важность аутентификации
- Виды аутентификации
- Пароль, биометрия, смарт карта...
- Проблемы аутентификации с помощью пароля
- Сложно ли внедрить двухфакторную аутентификацию?
- Требования для внедрения
- Демонстрация внедрения двухфакторной аутентификации.
- Подведем итоги...

Что такое аутентификация?

Основные понятия.

Процесс регистрации пользователя в системе состоит из трёх взаимосвязанных, последовательно выполняемых процедур: идентификации, аутентификации и авторизации.

- Идентификация – это процедура распознавания пользователя по его идентификатору.
- Аутентификация – процедура доказательства того, что пользователь на самом деле является тем, за кого он себя выдает.
- Авторизация – процедура предоставления пользователю определенных прав доступа к ресурсам системы.

Важность аутентификации

- Необходимо убедиться в том, что пользователь является тем, за кого он себя выдает.
- Необходимо убедиться в том, что устройство на другой стороне канала является «своим».
- Бессмысленно организовывать защищенный канал связи, если неизвестно кто находится с другой стороны канала.

Факторы аутентификации

- Для подтверждения своей подлинности, субъект должен предоставить некоторую секретную информацию, которая должна быть доступна только ему одному. Он может предъявлять системе различные виды информации.
- Фактор аутентификации — определенный вид информации, предоставляемый субъектом системе при его аутентификации.

Комбинация факторов

- Многофакторная аутентификация – аутентификация, в процессе которой используется несколько типов аутентификационных факторов.
- Метод аутентификации (метод регистрации) – специфика использования определенного типа аутентификационных факторов в процедуре аутентификации.
- Комбинация нескольких методов аутентификации, например, если служба аутентификации использует для аутентификации лицо и голос пользователя, не является многофакторной аутентификацией, так как оба используемых фактора относятся к одному типу аутентификационных факторов — «на основе биометрических данных».

Какие бывают факторы

- Иметь нечто (*дискету, токен,...*)
- Знать нечто (*пароль, логин,...*)
- Обладать некой биологической особенностью
(*отпечаток пальца, структура ДНК,...*)
- Находиться в определённом месте
(*IP-адрес, данные от радио-метки*)

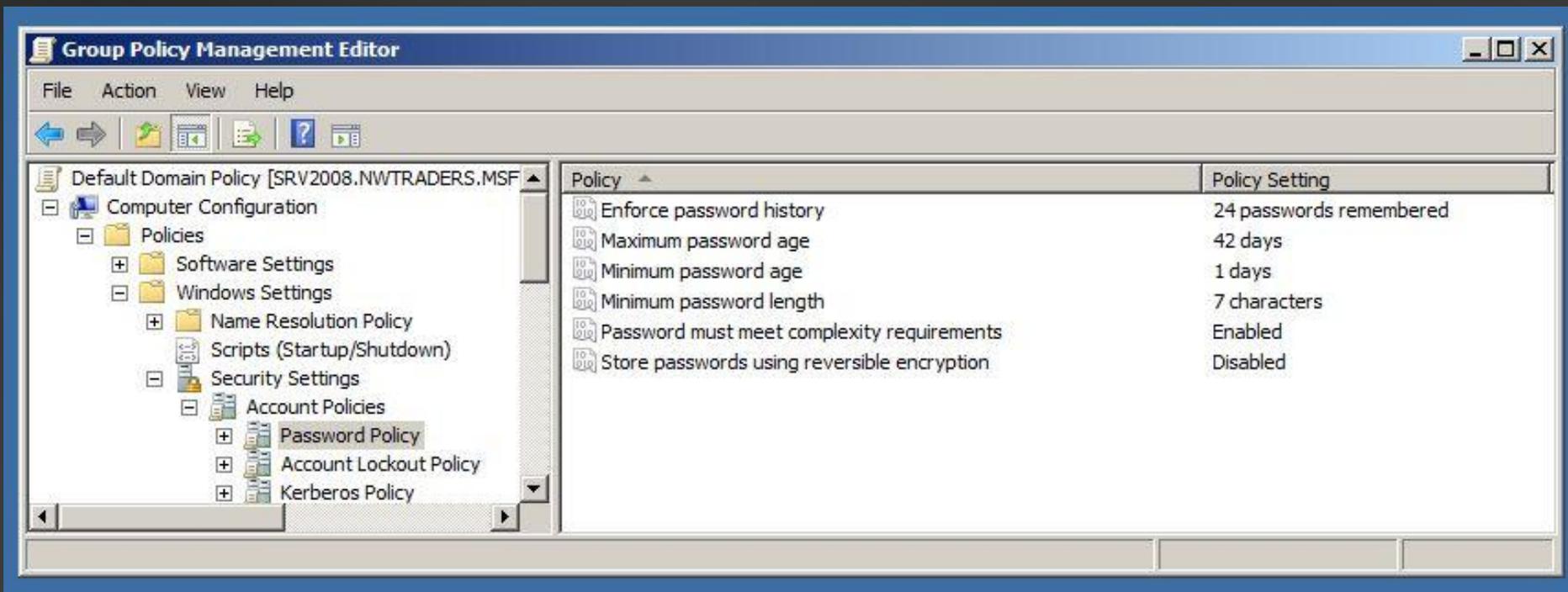
Аутентификация на основе пароля

- Просто реализовать
- Не требует инфраструктуры PKI
- Можно использовать политики для защиты

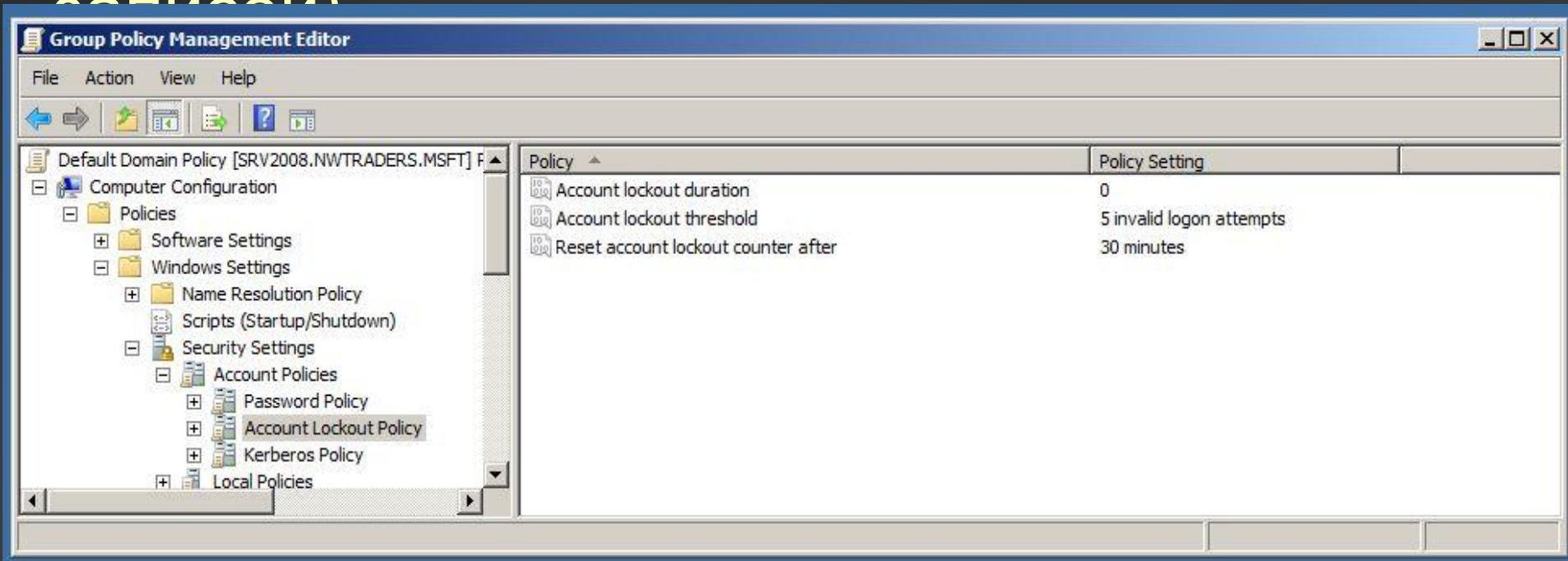
Некоторые методы взлома при использовании пароля

- Атака со словарем
- Угадывание пароля
- Социотехника
- Принуждение
- Подглядывание из-за плеча
- Троянский конь

Возможности защиты при аутентификации с помощью пароля (политика паролей)



Возможности защиты при аутентификации с помощью пароля (блокировки учетных записей)

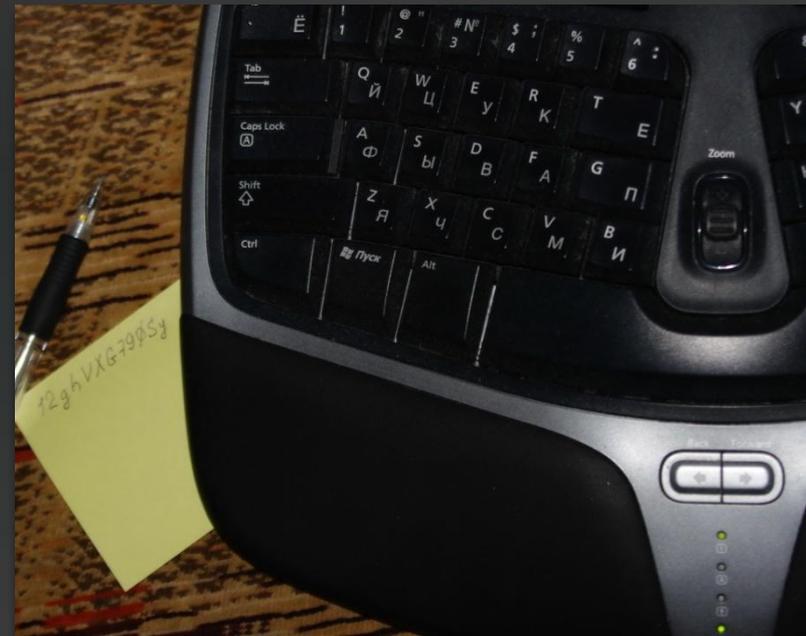
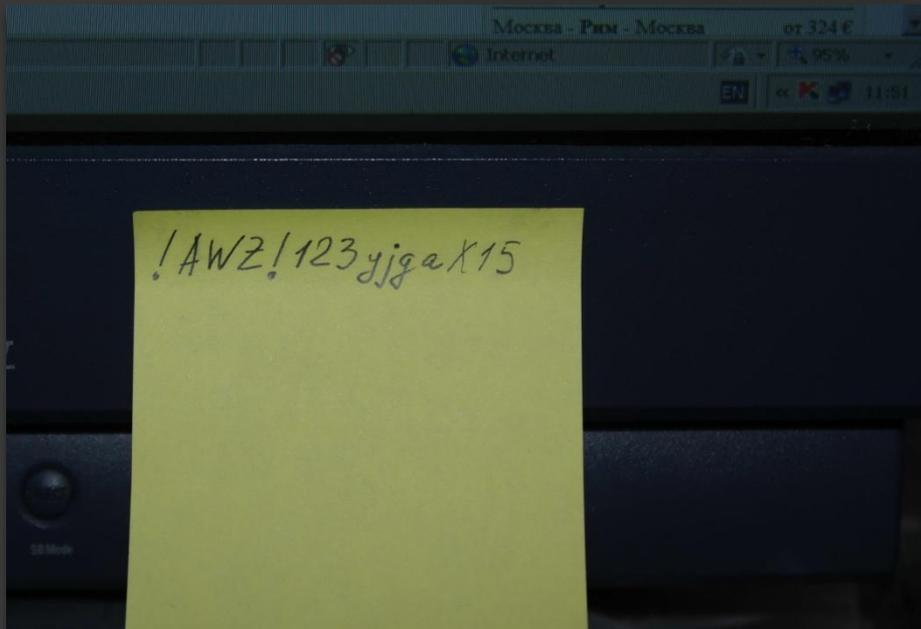


Когда не помогает сложный пароль?

- !AWZ!123yjgaX15
- 12ghVXG790Sy

Когда не помогает сложный пароль?

- !AWZ!123yjgaX15
- 12ghVXG790Sy



Что будем использовать?

- Двухфакторная аутентификация на основе смарт карт и USB – ключей
- RFID метки для разграничения физического доступа



Внедрение аутентификации на основе смарт карт

- Использование с AD DS
- Смарт карты и протокол Kerberos

Требования до ОС Windows Vista

- Доверие корневому УЦ
- CN=NTAuthCertificates, CN=Public Key Services, CN=Services, CN=Configuration, DC=nwtraders, DC=msft
- Smart Card Logon OID
- Client Authentication OID
- UPN
- Private key в защищенном хранилище
- Сертификат Domain Controller

Требования для Windows Vista и выше

- CRL Extension
- Certificate storage
- Manual mapping supported
- EKU extension

Изменения в поведении системы при входе клиента

- Ctrl+Alt+Delete
- Выбор сертификата для использования
- Lsass.exe

Подведем итоги...

- Аутентификация – это важно
- Аутентификация с использованием пароля, потенциально опасна
- Двухфакторная аутентификация – повышает безопасность
- Работает с AD и AD DS
- Какие произошли изменения

Сложно ли внедрить
аутентификацию с помощью смарт
карт и / или USB ключей в AD DS?

Как это будет работать с протоколом
Kerberos?

Как настроить Удостоверяющий Центр?
А что у нас есть в групповых политиках?

Настройка двухфакторной
аутентификации в AD DS с
помощью смарт карт и USB
ключей

Демонстрация

Леонид Шапиро
МСТ
ЦКО «Специалист»

компьютерного
Центр
ОБУЧЕНИЯ
«СПЕЦИАЛИСТ»
при МГТУ им. Н.Э.Баумана

Подведем итоги...

- Аутентификация и авторизация
- Надежная аутентификация – это важно
- Один или два фактора аутентификации
- Смарт карты и USB ключи – хорошее решение
- Внедрение для аутентификации в AD DS

Полезные материалы:

- 2821 Designing and Managing a Windows Public Key Infrastructure
- 2823 Implementing and Administering Security in a Microsoft Windows Server 2003 Network
- 2001В Построение структуры аутентификации в информационных системах на основе продуктов Aladdin
- 3001А Развертывание инфраструктуры открытых ключей. Использование смарт-карт и USB-ключей eToken.
- Microsoft Press Brian Komar «Windows Server 2008 PKI and Certificate Security»
- <http://technet.microsoft.com/en-us/library/dd277386.aspx>
- [http://technet.microsoft.com/en-us/library/dd367851\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd367851(WS.10).aspx)
- [http://technet.microsoft.com/en-us/library/cc721959\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc721959(WS.10).aspx)
- <http://www.specialist.ru/Security/#s112>

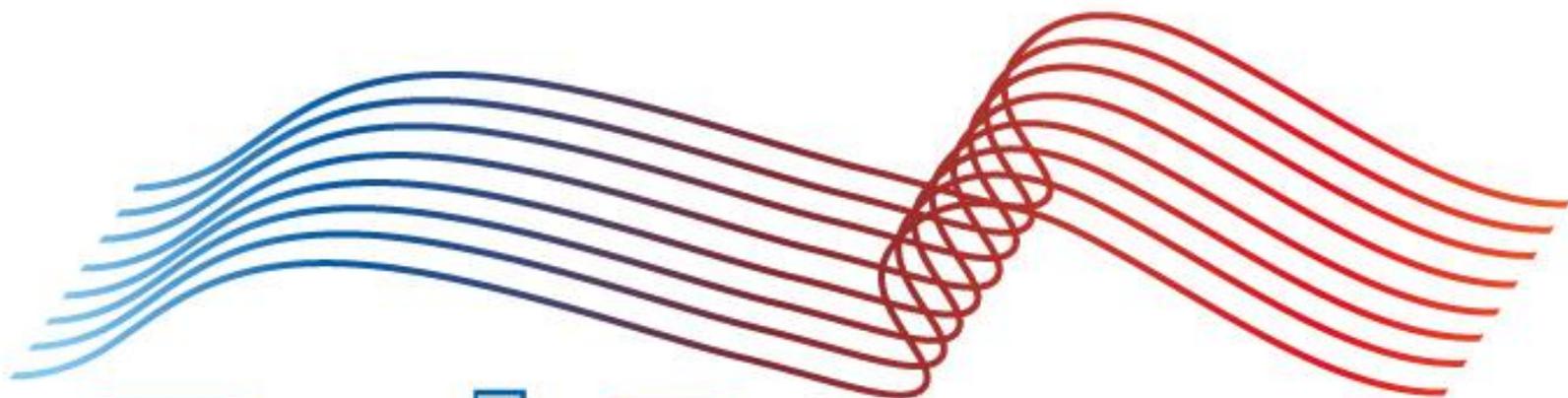
Microsoft[®]

Your potential. Our passion.[™]

© 2007 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries. The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.

Microsoft TechDays

<http://www.techdays.ru>



TechDays.ru