Jesper M. Johansson

with the Microsoft Security Team

Microsoft® Windows Server 2008™ Security Resourse Kit

Microsoft

Джеспер М. Джоханссон

совместно с Microsoft Security Team

Обеспечение безопасности

Ресурсы Windows Server® 2008

РУССКАЯ РЕДАКЦИЯ

BHV

Москва • 2009

УДК 681.3.06
ББК 32.973.26–018.2
Д42

Джоханссон Джеспер М.

Д42 Обеспечение безопасности. Ресурсы Windows Server® 2008. / Пер. с англ. — М. : Издательство «Русская Редакция» ; СПб. : БХВ-Петербург, 2009. — 544 стр. : ил.

ISBN 978-5-7502-0381-9 («Русская Редакция»)
ISBN 978-5-9775-0386-0 («БХВ-Петербург»)

Данное официальное руководство Microsoft содержит полное, углубленное описание планирования, развертывания и управления средствами обеспечения безопасности Windows Server 2008. В книге детально описаны новые инструменты безопасности Windows, объекты безопасности, сервисы безопасности, аутентификация пользователя и контроль доступа, стратегия сетевой безопасности и управление безопасной работой приложений, брандмауер Windows, безопасность ActiveDirectory, групповые политики, проведение аудита и управление обновлениями. На прилагаемом компакт-диске находятся полезные инструменты, готовые сценарии, шаблоны и другие полезные ресурсы.

Книга предназначена системным администраторам и опытным ИТ-специалистам крупных и средних компаний.

УДК 681.3.06
ББК 32.973.26–018.2

Джоханссон Джеспер М.

совместно с Microsoft Security Team

Обеспечение безопасности. Ресурсы Windows Server® 2008

Совместный проект издательства «Русская Редакция» и издательства «БХВ-Петербург».

РУССКАЯ РЕДАКЦИЯ bhv®

Подписано в печать 21.04.09. Формат 70×100/16. Физ. печ. л. 34
Тираж 1500. Заказ

Санитарно-эпидемиологическое заключение на продукцию
№ 77.99.60.953.Д.003650.04.08 от 14.04.2008 г. выдано Федеральной службой
по надзору в сфере защиты прав потребителей и благополучия человека.

Отпечатано с готовых диапозитивов
в ГУП «Типография «Наука»
199034, Санкт-Петербург, 9 линия, 12

ISBN 978-0-7356-2504-4 (англ.)
ISBN 978-5-7502-0381-9 («Русская Редакция»)
ISBN 978-5-9775-0386-0 («БХВ-Петербург»)

Краткое содержание

Оглавление

ЧАСТЬ II. Реализация контроля идентичности и доступа (IDA) с помощью службы Active Directory

ЧАСТЬ III. Стандартные сценарии безопасности

Об авторах

Эта книга была создана довольно оригинальным способом. Вместо одного человека, как обычно принято, ее писали 12 экспертов мирового класса, специализирующихся на безопасности сети. Серверы — вещь сложная, и Windows Server не исключение. Привлекая лучших специалистов из каждой области, мы смогли создать хорошую книгу по безопасности, в которой действительно содержатся полезные сведения, уже опробованные реальными людьми.

Джеспер М. Джоханссон (Jesper M. Johansson)

Джеспер М. Джоханссон выступил в качестве ведущего автора, разработал содержание и объединил авторский коллектив. Пока соавторы собирали вместе все то, что написали, Джеспер проверял, чтобы не была пропущена значимая информация.

Джеспер М. Джоханссон — известный специалист по информационной безопасности в общем и по безопасности Windows в частности. В настоящий момент он является главным разработчиком схемы безопасности программного обеспечения в компании Microsoft. До этого Джеспер работал над изданиями по безопасности в корпорации Microsoft, где описывались темы, начиная от взламывания сети до разработки программных средств безопасности. Джеспер читал лекции по главным проблемам безопасности на пяти континентах, написал множество соответствующих статей по этой теме и является наиболее ценным специалистом (MVP) по безопасности в Microsoft. Он обладает ученой степенью доктора философии в управленческих информационных системах и является сертифицированным специалистом по безопасности информационных систем (CISSP) и сертифицированным специалистом по архитектуре безопасности информационных систем (ISSAP). В свободное время Джеспер учит скуба-дайвингу.

Джимми Андерссон (Jimmy Andersson)

Джимми Андерссон является консультантом и главным советником в компании Q Advice AB в Швеции. Его направление — службы каталога. Он также работает преподавателем и разработал свой собственный курс по Active Directory (AD) под названием «Устранение неполадок AD и продвинутая теория». Корпорация Microsoft ежегодно на протяжении последних девяти лет присваивает ему звание MVP[1]. Обычно он выступает руководителем проекта по службам каталога в разработках крупных предприятий.

Сьюзен Брэдли (Susan Bradley)

Сьюзен работает с компьютерами с тех пор, как ее фирма впервые купила компьютер IBM 8088. Она работала в области обслуживания и планирования технологий своей компании и использовала собственные возможности в различных промышленных объединениях, разрабатывая лучшее и более безопасное программное обеспечение для малого бизнеса. Сьюзен пишет о выпусках обновлений программного обеспечения если не в блогах на sbsdiva.com, то на сайте WindowsSecrets.com. Кроме того, она призывает продавцов использовать более безопасный код с ее сайта threatcode.com. Ей нравится Windows Vista, и пока создавалась глава и материалы для этой книги, она ни разу не прибегала к подсказке управления учетной записью пользователя (UAC). Сьюзен является специалистом уровня MVP системы Windows Server для малого бизнеса.

Даррен Кэнэвор (Darren Canavor)

Даррен Кэнэвор — разработчик корпорации Microsoft. Он пришел в компанию в 1999 году и внес значительный вклад в проектирование безопасности и тестирование операционной системы Windows Core, включая инфраструктуру открытых ключей (PKI) в Windows 2000, службы сертификации в Windows Server 2003 и — совсем недавно — управление учетной записью пользователя в Windows Vista и Windows Server 2008. Даррен является соавтором множества технических описаний и книг Microsoft Press о безопасности и PKI корпорации Microsoft, например Windows Vista Security Guide

[1] Most Valuable Professionals — наиболее ценные профессионалы. Это самые авторитетные независимые специалисты по технологиям Microsoft, которые активно участвуют в форумах, User Groups, блогах, квалифицированно помогая другим пользователям продуктов Microsoft и программистам, создающим приложения на платформе Microsoft.

and Planning и Implementing Cross-Certification and Qualified Subordination Using Windows Server 2003.

Курт Диллард (Kurt Dillard)

Проживая в Буэнос-Айресе, солнечной столице Аргентины, Курт пишет книги и статьи, которые предлагают способы решения сложных задач защиты цифровой информации и хранящих ее компьютеров. Он работал над многими решениями, опубликованными корпорацией Microsoft, такими как «Windows Server 2003 Security Guide», «Security Risk Management Guide» и «Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP». Курт выступал на многочисленных конференциях, включая RSA, TechEd и федеральные саммиты по безопасности Microsoft. На сегодняшний день он обладает профессиональными сертификатами CISSP, ISSAP, CISM и MCSE: Security.

Эрик Фитцджеральд (Eric Fitzgerald)

Эрик (CISSP, MCSE) работает в отделении передовой продукции безопасности корпорации Microsoft, специализируясь на анализе данных от датчиков безопасности. Он провел шесть лет в команде безопасности операционной системы Windows Core, работая над технологиями аудита и авторизации в Windows, и несколько лет, обеспечивая поддержку клиентских предприятий корпорации Microsoft в области безопасности, сети и проблем со службой каталога. В свободное время Эрик наслаждается соревнованиями по гонкам на парусниках.

Роджер Граймс (Roger Grimes)

Роджер А. Граймс (обладатель сертификатов CPA, CISSP, CISA, MCSE: Security) — ветеран безопасности с 22-летним стажем, специализирующийся на безопасности хоста, PKI и управлении идентификацией. Роджер работает в команде ACE корпорации Microsoft в качестве старшего консультанта по безопасности. Он является обозревателем по безопасности сетей в журнале InfoWorld, а также автором и соавтором восьми книг по компьютерной безопасности. Кроме того, Роджер написал более 200 статей в журналы компании National Magazine. Он также продемонстрировал восемь вариантов приманок, фиксирующих хакерскую деятельность. Теперь Роджер ездит по всему миру, выступая на конференциях и объясняя покупателям, как стать максимально защищенными.

Байрон Хайнз (Byron Hynes)

Байрон Хайнз — стратег технологий предприятия в корпорации Microsoft. С тех пор как Хайнз пришел в компанию в 2005 году, он сконцентрировался на технологиях безопасности, включая функцию шифрования диска BitLocker, управление учетной записью пользователя и многое другое. Байрон работает непосредственно с покупателями, а также внес свой вклад в справочные файлы, сайты, статьи журналов, книг и презентаций. Ему очень нравится работать с людьми, и он встречается с покупателями настолько часто, насколько ему позволяет начальник. Байрон родился в Канаде и провел большую часть жизни в арктической зиме на севере. Теперь он живет в пригороде Редмонда, Вашингтон. Байрон женат и имеет двух сыновей.

Алан Джонс (Alun Jones)

Алан Джонс (специалист MVP, MCP) — президент компании Texas Imperial Software, которая разрабатывает программные средства для безопасности сети и обеспечивает службы инженерного консалтинга по безопасности. Ведущий продукт компании Texas Imperial Software — WFTPD Pro. Это безопасный FTP-сервер для Windows, полностью созданный Аланом.

Алан начал работать в области безопасности, когда все большая необходимость в поддержке WFTPD указывала на то, что не многие компании могут соответствовать требованиям по безопасности в Интернете без дополнительной помощи. На сегодняшний день он является разработчиком схем безопасности для интернет-компании, продающей книги, и специалистом MVP по безопасности Microsoft. Алан посещал лекции в университете в Корпус-Кристи-колледже, Кембридже и университете Бата. Сейчас живет возле Сиэтла, штат Вашингтон, со своей женой Дебби и сыном Колином. Алан благодарит жену и сына за их терпение во время его длительного отсутствия при написании этой книги.

Брайан Комар (Brian Komar)

Брайан Комар — президент компании IdentIT Inc., консалтинговой фирмы, специализирующейся на разработке инфраструктуры открытого ключа и на выполнении и решениях интеграции идентификации. Брайан является партнером корпорации Microsoft в нескольких предприятиях. Он создает обучающие материалы и технические описания по PKI и ILM 2007 и работает главным консультантом при развертывании на предприятиях PKI и ILM 2007. Брайан часто выступает на конференциях IT-индустрии, таких как Microsoft

TechEd, IT-форум Microsoft и встречах журнала Windows IT Pro. Брайан Комар является специалистом MVP по безопасности Microsoft.

Брайан Лич (Brian Lich)

Брайан Лич — центральный технический автор по безопасности в группе пользовательской поддержки Windows Server, пишущий о службах управления правами Active Directory. До прихода в корпорацию Microsoft он 11 лет работал в индустрии информационных технологий системным администратором и аналитиком по безопасности. У Брайана есть ученая степень по технологии электротехники, полученная в университете Пердью (Purdue University).

Даррен Мар-Элиа (Darren Mar-Elia)

Даррен Мар-Элиа — основатель и главный технический директор компании SDM Software, имеет очень большой опыт в разработке информационных технологий и программного обеспечения. Он был старшим директором отделения технической разработки товара в компании DesktopStandard (приобретенной корпорацией Microsoft), а до этого работал главным техническим директором в отделе решений управления Windows в корпорации Quest Software. Кроме того, был директором отдела распределенных систем в компании Charles Schwab & Co и руководил отделом по внедрению технологий Windows в этой компании. Даррен является автором и соавтором 12 книг на темы управления Windows и специалистом MVP групповой политики Microsoft. Он создал сайт gpoguy.com, на котором можно найти информацию по групповым политикам и утилиты для них.

Благодарности

Вне какой-либо очередности авторы хотели бы поблагодарить тех, кто помог в выпуске данного издания. Эти люди внесли неоценимый вклад в создание книги и помогли обеспечить ее соответствие высоким стандартам. Это Чейз Карпентер (Chase Carpenter), Аарон Маргозис (Aaron Margosis), Пол Янг (Paul Young), Пабло Ф. Матуте (Pablo F. Matute), Дана Эпп (Dana Epp), Чарли Рассел (Charlie Russel), Вольфган Шедлбауэр (Wolfgang Schedlbauer), Ник Гиллот (Nick Gillot), Стив Райли (Steve Riley), Джон Мишенер (John Michener), Грег Коттингам (Greg Cottingham), Остин Уилсон (Austin Wilson), Крис Блэк (Chris Black), Эд Уилсон (Ed Wilson), Эрин Бурк-Данпи (Erin Bourke-Dunphy), Кирк Солук (Kirk Soluk), Лара Сосновски (Lara Sosnosky), Ли Уокер (Lee Walker), Тал Сарид (Tal Sarid), Дэн Харман (Dan Harman), Ричард Б. Уорд (Richard B. Ward).

Кроме того, хотелось бы поблагодарить Митча Таллоха (Mitch Tulloch), нашего технического редактора, который прочитал всю книгу; Бекку Маккей (Becka McKay), нашего литературного редактора, выполнившую фантастическую работу и заставившую 12 голосов звучать как один; Девона Масгрейва (Devon Musgrave), который помог начать работу и обеспечил понимание того, что от нас ожидается; Морин Циммерман (Maureen Zimmerman), которая помогла окончить книгу и сделать это почти вовремя; и наконец, Мартина Дельри (Martin DelRe), который выполнил больше работы, чем ему было назначено, имея дело с 12 авторами.

Введение

Сейчас, держа в руках эту книгу, вы, уважаемый читатель, вероятно, чувствуете приятное волнение. Нет, не потому, что она закончена, а потому, что сам факт этого означает: появилась новая операционная система, которую можно исследовать! Даже если вы не из тех, кого волнуют подобные вещи, все равно вы держите в своих руках полный технический ресурс безопасности для операционной системы Windows Server 2008.

Windows Server 2008 — это модернизированная версия флагманской серверной операционной системы корпорации Microsoft. Значительные усилия были приложены не только для обеспечения ее высокого качества, но и для создания необходимых средств, которые гарантируют безопасное использование. Эта книга послужит вам компаньоном и помощником в изучении данных средств и определении способов их использования для предоставления лучших услуг или облегчения вашей жизни. Помимо этого, в книге исследуются те характерные особенности системы, описание которых ранее никогда не было доступно целевой аудитории – специалистам по информационным технологиям.

Издание содержит все технические детали, которых можно ожидать от полноценного комплекта ресурсов. Оно создано 12 экспертами мирового класса, каждый из которых признан ведущим специалистом в своей области. Они написали уже более 20 книг. Однако прежде всего являются специалистами в области информационных технологий.

Обзор книги

В книге 16 глав, которые разделены на три части.

- Часть I. Основы безопасности Windows.
  - **Глава 1. Субъекты, объекты и другие агенты.** В данной главе обсуждается, как в Windows происходит управление пользователями и другими субъектами.
  - **Глава 2. Аутентификаторы и протоколы аутентификации.** После своей идентификации субъект должен выполнить аутентификацию. Эта глава рассматривает работу аутентификации в Windows.
  - **Глава 3. Объекты: то, что вам нужно.** Пользователи обращаются к объектам, таким как файлы, разделы реестра и т. д. Это означает, что объекты должны быть защищены. В данной главе обсуждается, как это происходит.
  - **Глава 4. Контроль учетных записей пользователя (UAC).** Корпорация Microsoft внедрила контроль учетных записей пользователя (User Account Control, UAC) в Windows Vista. В первую очередь администраторы сервера должны понимать UAC для того, чтобы правильно управлять своими серве-

рами. Однако и тем, кто работает в более широкой области информационных технологий, необходимо знать, как использовать UAC для защиты сети. В этой главе мы расскажем, как это сделать.

- **Глава 5. Брандмауэр и защита доступа к сети.** Первичный брандмауэр в Windows — это брандмауэр Windows в режиме повышенной безопасности (Windows Firewall with Advanced Security). Данная глава посвящена его работе в Windows Server 2008.
- **Глава 6. Службы.** Когда процесс должен запускаться независимо от того, вошел ли пользователь в систему, этот процесс установлен как служба. Службы, следовательно, предоставляют значительное поле для атак на компьютерах, и поэтому важно понимать их влияние на безопасность.
- **Глава 7. Групповые политики.** При работе с сетями Windows ошибкой было бы не использовать групповые политики. Большинство модификаций защиты, создаваемой нами для систем, выполняется с использованием групповых политик.
- **Глава 8. Аудит.** Система безопасности не приносит большой пользы, если ее нельзя применять, чтобы доказать, кто и что делал. Аудит — фундаментальный компонент всей безопасности. В этой главе подробно рассказывается, как аудит работает в Windows.

- Часть II. Реализация контроля идентичности и доступа (IDA) с помощью службы Active Directory.
  - **Глава 9. Разработка доменных служб Active Directory для обеспечения безопасности.** Каждый может развернуть службу каталогов Active Directory, но, чтобы это действительно повышало безопасность сети, требуется умение. В данной главе описано, как это сделать.
  - **Глава 10. Реализация служб сертификации Active Directory.** Инфраструктуры открытых ключей (Public Key Infrastructures, PKI) многим видятся как ненужные усложнения. Ничто не может быть дальше от истины. Для многих (если не для большинства) сред они являются необходимым усложнением. В этой главе описаны нововведения в PKI для Windows Server 2008.
- Часть III. Стандартные сценарии безопасности.
  - **Глава 11. Роли сервера в организации безопасности.** Возможно, первое, что вы заметите в Windows Server 2008, — это исчезновение старых методов установки приложений. Вместо них появляется диспетчер серверов (Server Manager), который работает на основе ролевой модели. Из данной главы вы узнаете, как это влияет на безопасность и как использовать роли для защиты серверов.
  - **Глава 12. Управление обновлением.** К сожалению, каждый сервер время от времени требует обновлений. Программное обеспечение, будучи самой сложной вещью, когда-либо созданной человечеством, несовершенно. Управлять внесением исправлений непросто, но при наличии правильных инструментов и налаженного процесса вы можете значительно облегчить эту задачу.
  - **Глава 13. Организация безопасности сети.** Каждый компьютер находится в зависимости от чего-либо или кого-либо в вопросе безопасности. Грамотное управление этими зависимостями, вероятно, самое важное из того, что вы

можете сделать для защиты собственной сети. В этой главе мы обсуждаем зависимости, показываем, как провести моделирование угроз в вашей сети, и знакомим вас с одной из самых ценных на сегодня концепций безопасности: изоляцией сервера.

- **Глава 14. Организация безопасности филиала.** Одной из областей, в которых Windows Server 2008 предоставляет новые средства безопасности, являются сценарии филиала. Эта глава показывает, как воспользоваться каждым из них.
- **Глава 15. Размышления о малом бизнесе.** Windows Server 2008 предлагается в большем количестве вариантов, чем любая другая серверная операционная система, созданная компанией Microsoft. Две из них разработаны специально в соответствии с уникальными потребностями защиты для малого и среднего бизнеса. Если вы управляете сетью в компании малого бизнеса, эта глава будет для вас бесценным ресурсом.
- **Глава 16. Серверные приложения для организации безопасности.** Назначение большинства серверов — обеспечивать поддержку некоторых приложений. Хоть в этой книге мы не можем рассказать о каждом продукте, который может быть запущен на сервере, Microsoft поставляет платформу приложений IIS 7.0 вместе с Windows Server 2008. Эта глава поясняет, как управлять безопасностью данного компонента.

Смотрите дополнительную информацию в Интернете. По мере выхода нового материала, дополняющего эту книгу, он будет размещаться в Сети на сайте Microsoft Press Online Windows Server и Client. Основываясь на последней версии Windows Server 2008, материал, который там можно найти, включает обновления к содержанию книги, примеры глав, статьи, ссылки на сопровождающие материалы, опечатки и др. Сайт доступен по адресу: http://www.microsoft.com/learning/books/online/serverclient и периодически будет обновляться.

Условные обозначения

В данной книге используются следующие условные обозначения для выделения особых свойств или применения материала.

Вспомогательные средства

Здесь описываются вспомогательные средства, используемые в книге для выделения полезных деталей.

Выделяет особый случай, который может не подходить для каждой ситуации.

Подчеркивает важность определенной концепции.

Содержит полезную информацию по рассматриваемой теме, зачастую выделяя лучшие практические решения.

Привлекает внимание к главной информации, которая не должна быть пропущена.

Предупреждает вас, что невыполнение или непредотвращение выполнения обозначенного действия может вызвать серьезные проблемы для пользователей, систем, целостности данных и т. д.

Вставки

В книге используются вставки, представляющие дополнительную информацию, советы, рекомендации, касающиеся различных средств Windows Vista.

Прямо из первоисточника

Написана экспертами корпорации Microsoft или наиболее ценными специалистами (Most Valuable Professional, MVP) Microsoft для передачи более глубокого понимания работы Windows Vista, передового опыта управления безопасностью и советов по устранению неисправностей.

Как это работает

Предоставляет уникальный взгляд на средства Windows Server и их работу.

Ссылки на инструменты, обсуждаемые в книге

Вместо того чтобы дать вам версии загружаемых инструментов, которые становятся устаревшими, как только вы покупаете книгу, мы предлагаем ссылки на инструменты для загрузки, которые обсуждаются в книге или которые просто полезно иметь.

- Windows PowerShell — это новая командная оболочка и сопутствующий язык сценариев, разработанные для системного администрирования и автоматизации. Построенная на базе .NET, оболочка Windows PowerShell позволяет IT-специалистам и разработчикам управлять и автоматизировать процессы администрирования для Windows и приложений.

  Оболочка Windows PowerShell для Windows Vista версий x64 доступна в Интернете по следующим адресам: http://www.microsoft.com/downloads/details.aspx?FamilyID=c6ef4735-c7de-46a2-997a-ea58fdfcba63&DisplayLang=en и http://www.microsoft.com/downloads/details.aspx?FamilyID=af37d87d-5de6-4af1-80f4-740f625cd084&DisplayLang=en.

- Process Explorer — это отличный инструмент, позволяющий узнать больше о том, что происходит на вашем компьютере, чем вы когда-либо могли мечтать.

  Process Explorer можно скачать в Интернете по адресу http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx.

- Microsoft Network Monitor — это чрезвычайно мощный и полезный инструмент управления сетью и устранения неисправностей. Он позволяет нам видеть весь входящий и исходящий сетевой трафик. Это обязательный инструмент в арсенале любого администратора.

  Microsoft Network Monitor доступен для скачивания в Интернете по адресу http://www.microsoft.com/downloads/details.aspx?FamilyID=f4db40af-1e08-4a21-a26b-ec2f4dc4190d&displaylang=en.

- Privbar — это инструмент для Проводника Windows и Internet Explorer, показывающий, являетесь вы администратором или обычным пользователем.

  Privbar доступен в Интернете по адресу http://blogs.msdn.com/aaron_margosis/archive/2004/07/24/195350.aspx.

Политика поддержки комплекта ресурсов

Нами были предприняты все усилия, чтобы избежать ошибок, неточностей и опечаток в книге. Microsoft Press предлагает исправления к книге, доступные в Интернете по следующему адресу: http://www.microsoft.com/learning/support/search.asp.

Если у вас есть комментарии или идеи касательно содержимого этой книги либо если у возникли вопросы, на которые не нашлось ответов в Базе знаний, пожалуйста, пришлите их в Microsoft Press, используя один из следующих способов:

- с помощью электронной почты: rkinput@microsoft.com;
- по обычной почте:

  Microsoft Press

  Attn: Microsoft Windows Server 2008 Security Resource Kit

  One Microsoft Way

  Redmond, WA 98052-6399.

Обратите внимание на то, что поддержка продукта по вышеуказанным адресам не предусмотрена. За информацией по поддержке продукта обращайтесь на сайт Microsoft по адресу http://support.microsoft.com.

Дополнительные материалы

По просьбе распространителей данной книги дополнительные материалы, размещенные на компакт-диске оригинального издания, находятся на сайте издательства «Русская Редакция» по адресу http://rusedit.com/downloads/WRS/.

От издательства

Ваши замечания, предложения и вопросы отправляйте по адресу электронной почты dgurski@minsk.piter.com (издательство «Питер», компьютерная редакция).

Мы будем рады узнать ваше мнение!

На сайте издательства http://www.piter.com вы найдете подробную информацию о наших книгах.

ЧАСТЬ I

Основы безопасности Windows

ГЛАВА 1

Субъекты, объекты и другие агенты

Джеспер М. Джоханссон

На самом элементарном уровне в вопросе безопасности все сводится к объектам и субъектам. Объекты — это то, что мы защищаем, а субъекты — это те, от кого мы защищаем объекты. Субъекты и объекты используются в аутентификации (доказательстве нашей личности), авторизации (получении доступа к чему-либо) и аудите (отслеживании, кто к чему получал доступ). Эти концепции фундаментально очень просты. Субъекты — это пользователи. Объекты — это файлы. Аутентификация, авторизация и аудит относятся к взаимоотношениям субъектов и объектов. Так было, а в некоторых простых системах так все еще есть.

В Windows, однако, поддерживается чрезвычайно богатая семантика в том, что касается безопасности, и очень сильно расширены определения субъекта и объекта. Понятие субъекта намного шире, чем определение его как просто пользователя, и его представление намного сложнее, чем просто элементарный идентификатор пользователя. В Windows они даже называются по-разному. Мы очень часто будем применять термин «принципал безопасности». На языке Windows «принципал безопасности» означает не только типичного субъекта (о котором мы бы подумали, что это пользователь), но также группы и компьютеры. Принципал безопасности — это все, кому может быть назначен идентификатор безопасности (Security Identifier, SID) и кому может быть дано разрешение на доступ к чему-либо. Из этой главы вы узнаете о различных субъектах, которые могут быть принципалами безопасности, и о том, как они идентифицируются в операционных системах Windows в целом, а также о нововведениях в Windows Server 2008. В гл. 3 речь пойдет о другой стороне безопасности — объектах.

Субъект/объект/операция-кортеж

Управление безопасностью очень часто сводится к схеме «субъект/объект/операция-кортеж». Субъект — это агент, который пытается выполнить какое-либо действие с объектом. Например, пользователь может пытаться получить доступ к файлу, как показано на рис. 1.1.

Когда пользователь пытается прочитать файл, операционная система проверяет, имеются ли права доступа к объекту (файлу), которые позволяют субъекту (пользователю) выполнить действие. Если у пользователя есть права доступа к файлу, то его запрос на доступ удовлетворяется. Если права доступа не включают требуемых субъекту прав, то его запрос на доступ отклоняется. До сих пор все очень просто.

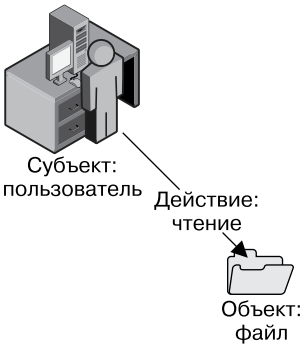

Рис. 1.1. Пользователь пытается прочитать файл

В гл. 3 мы поговорим больше о том, как работают права доступа и как осуществляется процесс проверки доступа. В этой главе мы остановимся на идентификации субъекта. Как было сказано ранее, различные действующие лица могут считаться субъектами. В большинстве ситуаций — это пользователи, но так бывает не всегда. В следующем разделе будут рассмотрены типы субъектов и то, как они представлены в Windows.

Типы принципалов безопасности

Субъектами, или, как мы их будем с этого момента называть, принципалами безопасности, в системе на базе Windows и, следовательно, в сети на базе Windows могут быть различные лица — не только пользователи. Однако пользователь все равно остается основным участником.

Пользователи

Пользователь — это определенное лицо, которое выполняет вход в компьютер. Фундаментально принципалы безопасности каким-то образом являются пользователями.

В Windows может быть два типа пользователей: локальные и доменные. Локальный пользователь определяется на компьютере в локальной базе данных диспетчера учетных записей безопасности (Security Accounts Manager, SAM). Каждый компьютер на базе Windows имеет локальный SAM, который ведет учет всех пользователей этого компьютера.

Хотя все операционные системы на базе Windows NT поддерживают какие-то основные структуры безопасности, в серверных версиях, начиная с Windows 2000, служба каталогов Active Directory поддерживает набор функций, намного отличающийся от возможностей клиентских версий и предыдущих версий Windows NT.

С этого момента, когда в книге встречаются выражения «компьютер на базе Windows» или «Windows», имеются в виду компьютеры с линейкой операционных систем Windows NT. Она включает: Windows NT 3.1/3.5/3.51/4.0, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008.

Принято думать, что контроллеры домена (DC) не имеют локального диспетчера учетных записей безопасности (SAM) и, следовательно, локальных пользователей. Это неправильно. Даже DC имеет локальный SAM, но учетные записи в его SAM могут использоваться только в режиме восстановления службы каталогов (DSRM). По умолчанию две учетные записи пользователей всегда есть в локальном SAM: Administrator (Администратор) и Guest (Гость). Учетная запись Guest (Гость) по умолчанию отключена.

Когда мы пишем Administrator (Администратор) или Administrators (Администраторы), то говорим соответственно о пользователе или о группе. Когда мы пишем «администратор» со строчной буквы, говорим об учетной записи некоторого пользователя или о человеке, имеющем права администратора. То же касается таких пользователей, как Guest (Гость) и гость.

В Windows Server 2008 учетная запись администратора активна по умолчанию и является учетной записью, которую необходимо использовать, чтобы подключиться к компьютеру в первый раз. В Windows Vista учетная запись администратора отключена по умолчанию и может использоваться только при особых обстоятельствах. В обоих случаях настоятельно рекомендуется создать дополнительные учетные записи для каждого пользователя, который будет администрировать данный компьютер. При необходимости выполнения каких-либо правил это становится требованием: одна учетная запись должна быть собственной персональной административной учетной записью каждого пользователя. Если администраторы используют компьютер не для целей администрирования, они должны иметь персональные неадминистративные учетные записи.

Другой тип учетной записи — доменная. Она определяется на контроллере домена (DC) для домена и может использоваться на любом компьютере домена. Доменные учетные записи могут иметь значительно большее количество свойств по сравнению с локальной учетной записью. Сравним рис. 1.2 и 1.3.

Доменные учетные записи имеют более богатую семантику, охватывающую множество атрибутов в организационной среде, таких как телефонные номера, управленческие взаимоотношения, адреса электронной почты и т. д. Доменные учетные записи также более полезны в сети, поскольку их можно использовать и назначать им права на компьютерах во всей сети. Назначение учетных записей в домене также упрощает управление. Чтобы больше узнать о службе каталогов Active Directory, смотрите гл. 9.

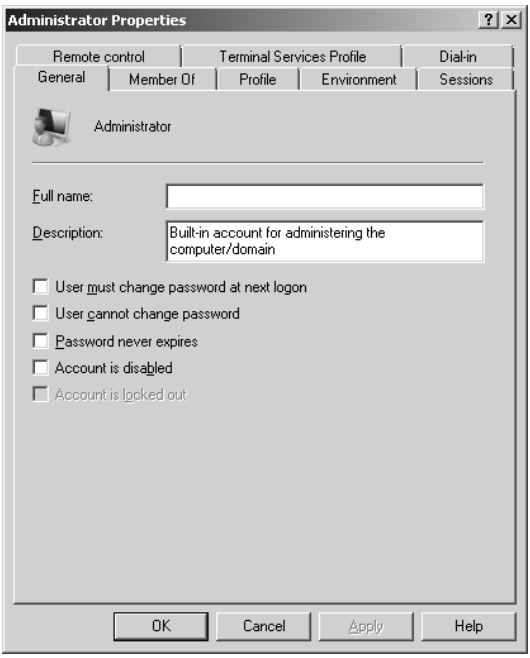

Рис. 1.2. Окно свойств локальной учетной записи

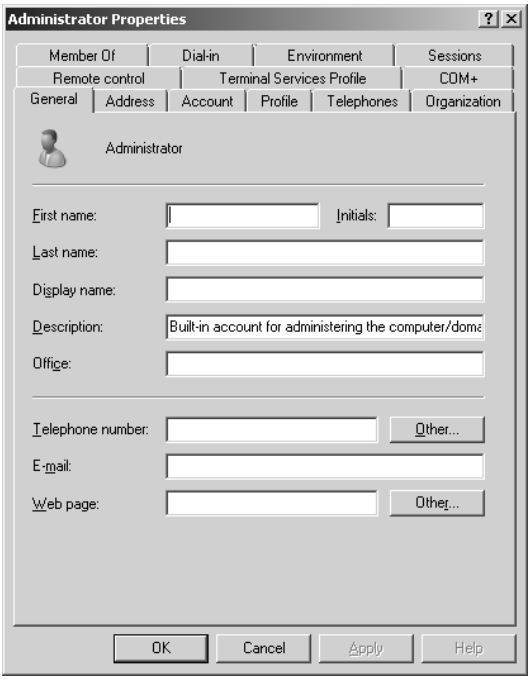

Рис. 1.3. Окно свойств доменной учетной записи

Компьютеры

Компьютер — это всего лишь еще один тип пользователя. В службе каталогов Active Directory это особенно заметно и подтверждается моделью наследования. Структура наследования, ведущая к компьютеру, показана на рис. 1.4.

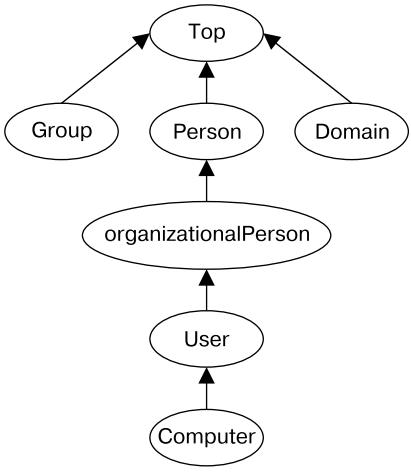

Рис. 1.4. Иерархия наследования в службе каталогов Active Directory показывает, как соотносятся пользователи и компьютеры

На рис. 1.4 можно заметить несколько интересных вещей. Во-первых, все классы в службе каталогов Active Directory происходят из корневого класса, который называется `Top`. На самом же деле даже `Top` указан как подкласс `Top`. Во-вторых, класс `User` происходит от класса `organizationalPerson`. Класс `organizationalPerson` происходит от `Top`. И наконец, самая интересная часть — класс `Computer` — происходит от класса `User`. Другими словами, на языке объектного ориентирования `Computer` — это тип пользователя. Это кажущееся «очеловечивание» компьютеров имеет большой смысл, поскольку компьютеры нужно рассматривать еще и как с субъекты и они имеют почти те же атрибуты, что и пользователи.

Группы

Субъект, как вы помните, — это некто, кто пытается получить доступ к объекту. Операционная система верифицирует эту попытку доступа путем проверки прав доступа к данному объекту. Очень быстро разработчики операционных систем поняли, что будет чересчур объемным назначать права доступа на каждый объект каждому пользователю, который в нем нуждается. Чтобы разрешить эту проблему, они позволили пользователям быть членами групп. Это дает нам возможность назначать права группам в дополнение к назначению прав пользователям. Группа может не быть пользователем, но она все равно является типом принципала безопасности, поскольку может иметь идентификатор, так же как пользователи и компьютеры. В Windows пользователь может быть членом многих групп, и на доступ

к объекту могут иметься права, назначенные различным группам. Вложенные группы также допустимы, но имеются некоторые ограничения.

Недоменный контроллер имеет только два вида групп: встроенные и локальные, которые определил администратор. В службе каталогов Active Directory, однако, есть шесть видов групп безопасности: встроенная доменная локальная, глобальная и универсальная группы и определяемые пользователем доменная локальная, глобальная и универсальная группы.

Доменным локальным группам могут назначаться права доступа только на ресурсы в том домене, в котором они определены, но они могут включать пользователей, универсальные и глобальные группы из любого доверяемого домена или леса, а также доменные локальные группы из собственного домена.

Глобальная группа может включать только пользователей и глобальные группы из того домена, в котором была определена, но ей могут быть назначены права доступа на ресурсы в любом домене в том лесу, частью которого этот домен является, или в любом доверяющем лесу.

Универсальная группа может включать пользователей и универсальные и глобальные группы из любого домена. Универсальной группе могут быть назначены права доступа к ресурсам в любом доверяющем домене или лесу (рис. 1.5).

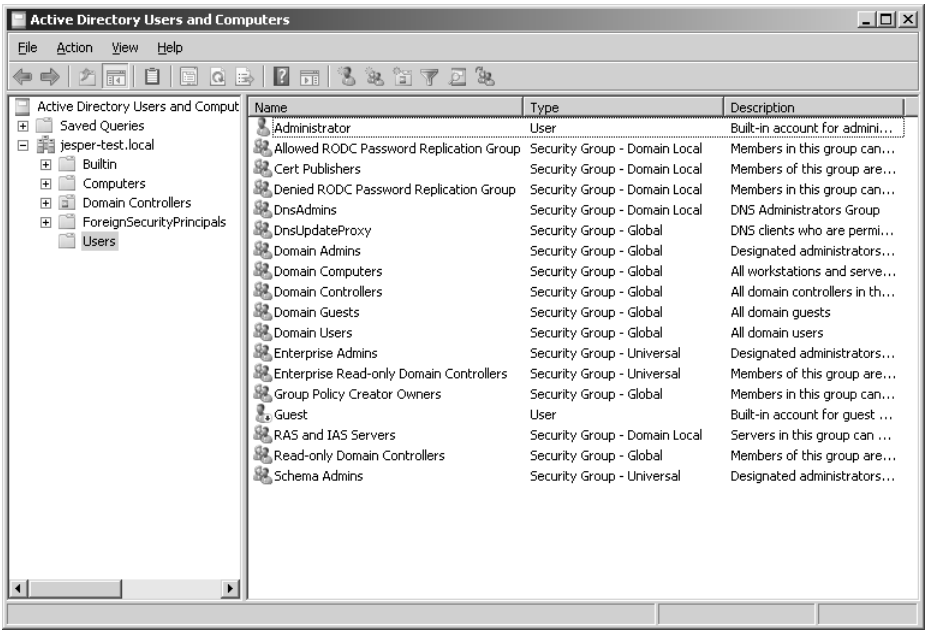

Рис. 1.5. Значительное количество групп определено в контейнере Users (Пользователи) в службе каталогов Active Directory по умолчанию

В то время как рядовой сервер по умолчанию имеет только две группы (Administrators (Администраторы) и Guests (Гости)), домен имеет большее количество всех трех типов. Рисунок 1.5 показывает группы по умолчанию в домене. Все

они являются группами безопасности, а это значит, что им могут быть назначены права доступа. Группы безопасности не стоит путать с группами распределения, которые используются на сервере Microsoft Exchange Server для объединения пользователей в группы таким образом, чтобы можно было послать электронное сообщение группе людей. Обе группы определены в службе каталогов Active Directory.

В дополнение к группам, определенным в домене, которые существуют только в доменах, также имеются встроенные локальные группы. Это группы, определенные в отличной от доменных групп иерархии, обладающие другими полномочиями. Встроенные группы не являются доменными группами как таковыми, а скорее встроены на всех или, по крайней мере, на некоторых компьютерах на базе Windows вне зависимости от того, являются ли они контроллерами домена. Они существуют на всех компьютерах на базе Windows, но определяются в службе каталогов AD на контроллере домена (DC). Например, группа Administrators (Администраторы) — это встроенная группа, которая существует на всех компьютерах на базе Windows, в то время как группа Domain Admins (Доменные администраторы) — это доменная группа, которая существует только в доменах. Рис. 1.6 показывает 21 встроенную группу на тестовом компьютере.

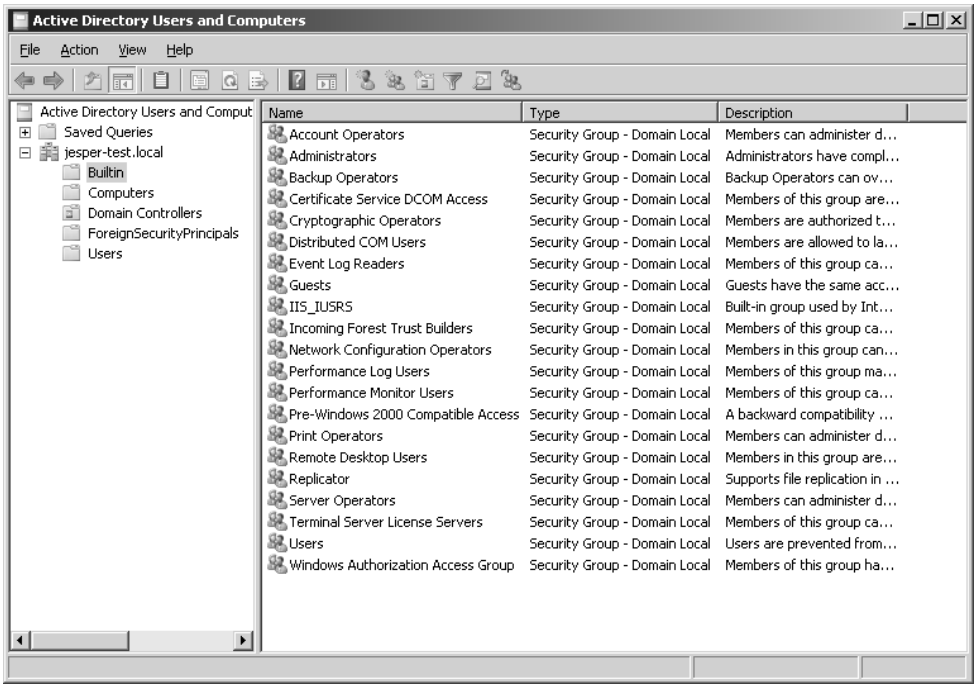

Рис. 1.6. Дополнительные группы — это так называемые встроенные группы

Однако при попытке назначить права доступа к объекту мы бы обнаружили еще больше групп. На самом деле на стандартном DC мы бы увидели не менее 63 (!) групп и встроенных принципалов безопасности (рис. 1.7).

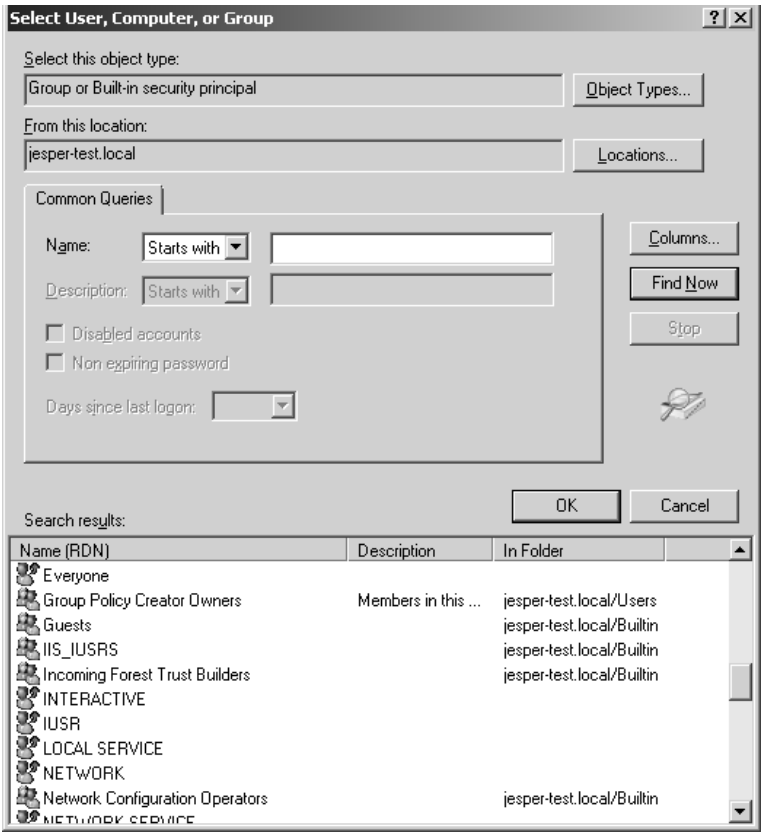

Рис. 1.7. На DC вы найдете не менее 63 групп и встроенных принципалов безопасности

Дополнительные 26 групп являются абстрактными понятиями, представляющими динамическую группу принципалов безопасности. Их обычно называют особыми объединениями (special identities).

Абстрактные понятия (группы регистрации в системе)

В дополнение к реальным группам, которые мы задаем на компьютере, существуют также и другие группы (см. рис. 1.7). Это группы, которые представляют какой-либо динамический аспект принципала безопасности, вроде того, каким образом пользователь или другой принципал безопасности подключен к сети. Например, группа INTERACTIVE, показанная на рис. 1.7, включает всех пользователей, подключенных к консоли компьютера через терминальные сервисы. Напротив, группа NETWORK включает всех пользователей, подключенных через сеть. По определению пользователь может быть членом только одной из этих групп одновременно и членство в них назначается в момент входа в систему. Вы можете использовать данные

группы для предоставления прав доступа всем пользователям, которые входят в систему тем или иным способом.

Можно увидеть и другие группы подобного рода. Особо стоит отметить Everyone (Все пользователи) и Authenticated Users (Аутентифицированные пользователи). Группа Everyone (Все пользователи) включает, как следует из названия, всех подключенных к компьютеру пользователей, кроме исключаемых начиная с Windows XP полностью анонимных пользователей. Подчеркну, что пользователи с учетной записью «гость» включены в эту группу. Группа Authenticated Users (Аутентифицированные пользователи), также заполняемая динамически, включает только аутентифицированных пользователей. Это означает, что гости не включены в группу Authenticated Users (Аутентифицированные пользователи). Это и есть единственное отличие рассматриваемых групп. Поскольку единственная гостевая учетная запись, существующая в операционной системе, отключена, нет функционального различия между Authenticated Users (Аутентифицированные пользователи) и Everyone (Все пользователи), если только мы не активировали учетную запись «гость» вручную. Несмотря на это, многие администраторы теряли долгие часы сна, думая о том, что все на свете имеют права доступа на их сервер, и предпринимали радикальные меры, чтобы модифицировать права доступа для исправления этой ситуации. Обычно такие изменения имеют катастрофические последствия. Да и нет абсолютно никакой причины производить подобные действия. Либо мы хотим, чтобы гости имели права доступа на наш компьютер, и активируем гостевую учетную запись, либо нет, и тогда оставляем ее отключенной. Если мы хотим, чтобы у гостей были права доступа, нам нужны права доступа для группы Everyone (Все пользователи). Если нет, эта группа не будет ничем отличаться от группы Authenticated Users (Аутентифицированные пользователи).

Некоторые утверждают, что данные изменения являются дополнительным уровнем защиты. Это было бы так, если бы мы могли определить дополнительную защиту как изменения, которые не можем оправдать другим способом. Факт же состоит в том, что эти изменения дают очень слабую защиту и несут очень большой риск. Оставьте установки по умолчанию в покое. Если это звучит недостаточно убедительно, то вам следует обратиться к статье 885409 Базы знаний Microsoft, в которой говорится, что массовая замена прав доступа может привести к недействительности контракта о поддержке. Когда вы заменяете права доступа, вы, по сути, создаете свою собственную операционную систему, и корпорация Microsoft не может больше гарантировать, что она будет работать.

Стоит также указать на разницу между группой Users (Пользователи), которая является встроенной, и группой Authenticated Users (Аутентифицированные пользователи). Различие здесь состоит в том, что группа Authenticated Users (Аутентифицированные пользователи) включает каждого пользователя, который аутентифицировался на компьютере: пользователей в различных доменах, пользователей — членов локальных групп, кроме группы Users (Пользователи), и пользователей, не являющихся членами каких-либо групп вообще (да, такое возможно). Другими словами, группа Users (Пользователи) накладывает гораздо больше ограничений, чем группа Authenticated Users (Аутентифицированные пользователи).

Вопреки этому, я видел многие организации, которые, пытаясь укрепить свои системы, заменяли права доступа для Users (Пользователи) правами доступа для Authenticated Users (Аутентифицированные пользователи). Стоит ли говорить, что эти попытки были безуспешны с точки зрения как безопасности системы, так и особенно ее стабильности.

Службы

Непрекращающиеся дебаты вокруг брандмауэров на базе хоста длятся долгие годы. Одна часть спорящих, активно поддерживаемая продавцами таких продуктов, доказывает, что брандмауэры на базе хоста фильтруют исходящий трафик и таким образом защищают остальную сеть от зараженного компьютера. Более объективные умы утверждают, что если компьютер заражен, то вредоносные программы уже присутствуют на нем и могут обойти или полностью отключить брандмауэр на базе хоста. Конечно, если вредоносное программное обеспечение попало на компьютер, заразив какое-то приложение, которое запускалось с минимальными привилегиями, этот довод не выдерживает критики. В последние годы корпорация Microsoft потратила значительное количество времени на то, чтобы службы могли работать с более низкими привилегиями. Но служба, работающая как конкретный пользователь, все равно могла управлять любой службой, работающей как тот же пользователь, и могла делать все, что могла делать управляемая служба. Так, если бы служба A могла отправить трафик через брандмауэр, а служба B — нет, то служба B могла бы получить контроль над службой A и отправить трафик в то время, когда они работали как один и тот же пользователь.

Для решения этой проблемы корпорация Microsoft нуждалась в способе назначения прав процессу, или, точнее, службе. Для этого, начиная с Windows Vista и Windows Server 2008, службы превратили в полноправные принципалы безопасности. Теперь каждая служба имеет идентификатор, который может быть использован для назначения ему полномочий. Помечая полномочия для этого идентификатора как ограниченные (см. гл. 3 для получения более подробной информации о записях в списке ограниченного доступа), мы даже можем обеспечить, чтобы конкретный принципал безопасности был в наличии при подаче запроса, независимо от того, какие другие права доступа перечислены для объекта. Затем для некоторых ситуаций появился смысл использовать исходящие фильтры брандмауэров на базе хоста, поэтому брандмауэр в Windows Vista и Windows Server 2008 теперь их поддерживает. По умолчанию он блокирует исходящий трафик от служб, за исключением тех портов, которые требуются этим службам. Это, честно говоря, максимум безопасности, которой можно ожидать от брандмауэра на базе хоста.

Идентификаторы безопасности

До сих пор мы обходили тему идентификаторов. Я упоминал ранее, что принципал безопасности — это субъект, который может иметь идентификатор безопасности (SID), но не дал определения идентификатору безопасности.

В общем под идентификатором безопасности понимают числовое представление принципала безопасности. Идентификатор SID используется внутри операционной системы: когда мы предоставляем пользователю, группе, службе или другому принципалу безопасности права доступа к объекту, операционная система записывает идентификатор SID и права доступа в список контроля доступа (Access Control List, ACL).

Компоненты идентификатора SID

Идентификатор безопасности состоит из нескольких обязательных элементов. На рис. 1.8 показаны различные компоненты идентификатора SID.

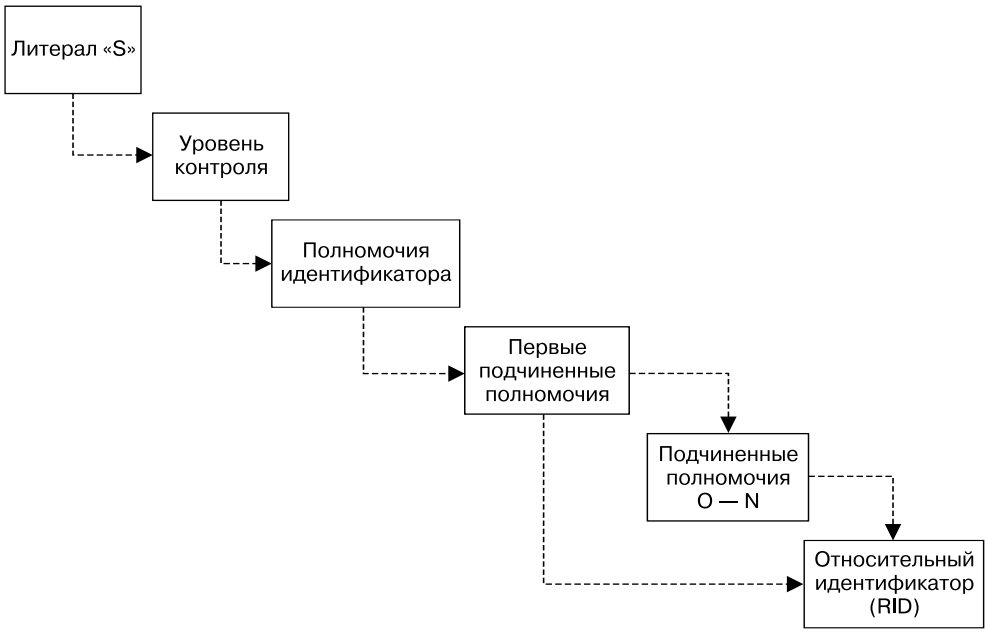

Рис. 1.8. Идентификатор SID имеет определенную структуру с несколькими обязательными элементами

Идентификаторы SID всегда начинаются буквой S, которая определяет их как SID. Они также всегда заканчиваются относительным идентификатором (Relative Identifier, RID). Между ними находятся 0 или более подчиненных полномочий. Второе значение в SID — это уровень контроля, который в настоящее время всегда равен 1.

Полномочия идентификатора SID

После префикса S-1 остальная часть идентификатора SID может значительно отличаться, но она всегда начинается с полномочий идентификатора, обозначающих субъекта, который их присвоил. В табл. 1.1 показаны используемые в настоящее время полномочия идентификатора.

Таблица 1.1. Полномочия идентификатора SID

Полномочия идентификатора	Описание
0	SECURITY_NULL_SID_AUTHORITY — используются для сравнений, когда неизвестны полномочия идентификатора
1	SECURITY_WORLD_SID_AUTHORITY — применяются для конструирования идентификаторов SID, которые представляют всех пользователей. Например, идентификатор SID для группы Everyone (Все пользователи) — это S-1-1-0. Он создается добавлением WORLD RID (0) к полномочиям этого идентификатора, выбирая, таким образом, всех пользователей из этих полномочий
2	SECURITY_LOCAL_SID_AUTHORITY — используются для построения идентификаторов SID, представляющих пользователей, которые входят на локальный терминал
3	SECURITY_CREATOR_SID_AUTHORITY — применяются для создания идентификаторов SID, представляющих создателя или владельца объекта. Например, CREATOR OWNER SID выглядит как S-1-3-0. Он создан путем добавления относительного идентификатора создателя или владельца (равен 0) к полномочиям рассматриваемого идентификатора. Если идентификатор S-1-3-0 используется в наследуемом списке контроля доступа (ACL), то он будет заменен идентификатором SID владельца в дочерних объектах, которые наследуют этот ACL. Таким образом, SID группы CREATOR GROUP (группы создателя) будет выглядеть как S-1-3-1. Он выполняет те же функции, что и идентификатор S-1-3-0, но вместо этого примет SID для первичной группы создателя
5	SECURITY_NT_AUTHORITY — это сама операционная система. Идентификаторы SID, которые начинаются с S-1-5, выпущены компьютером или доменом. Большинство идентификаторов SID, которые мы будем встречать, начинаются с S-1-5

Прямо из источника: история идентификатора SID

В первоначальной концепции идентификатора SID вызывался каждый уровень иерархии. Каждый уровень включал подчиненные полномочия, и организация могла выставить иерархии полномочий произвольного уровня сложности. Каждый уровень мог, в свою очередь, создавать дополнительные полномочия ниже. В реальности это создавало большие трудности при установке и использовании и делало группу модели управления слишком запутанной. Концепция идентичностей произвольной глубины потеряла жизнеспособность уже на ранней стадии своего развития, однако структура была уже слишком глубоко укоренена, чтобы ее можно было изъять.

Практика выработала два шаблона идентификатора SID. Для встроенных, предопределенных структур иерархия была сжата до глубины в 2 или 3 подчиненных полномочия. Для настоящих идентичностей других принципалов полномочия идентификатора были установлены равными 5, а набор подчиненных полномочий был установлен равным 4.

Ричард Б. Уорд, архитектор Windows Core

После полномочий идентификатора в SID есть некоторое количество подчиненных полномочий. Последнее из них называется относительным идентификатором и является идентификатором уникального принципала безопасности в области, в которой был определен SID.

Для примера рассмотрим следующий идентификатор SID: S-1-5-21-1534169462-1651380828-111620651-500. Как видим, идентификатор SID начинается с S-1-5, что указывает на его создание Windows NT. Первые подчиненные полномочия равны 21 (0x15 в шестнадцатеричной системе счисления). Значение 21 определяет этот идентификатор как идентификатор SID Windows NT, который не является уникальным в глобальном масштабе. Он будет уникален внутри домена, где был издан, но в мире компьютеров могут быть другие идентификаторы SID, имеющие точно такое же значение. Первые из подчиненных полномочий очень часто являются общеизвестными. В табл. 1.2 перечислены наиболее часто встречаемые общеизвестные подчиненные полномочия.

Таблица 1.2. Общеизвестные подчиненные полномочия

Подчиненные полномочия	Описание
5	Идентификаторы SID присваиваются сеансам регистрации для выдачи прав любому приложению, запускаемому во время определенного сеанса регистрации. У таких идентификаторов SID первые подчиненные полномочия установлены как 5 и принимают форму S-1-5-5-x-y
6	Когда процесс регистрируется как служба, он получает специальный идентификатор SID в свой маркер для обозначения данного действия. Этот идентификатор SID имеет подчиненные полномочия 6 и всегда будет S-1-5-6
21	SECURITY_NT_NON_UNIQUE — обозначают идентификатор SID пользователя и идентификатор SID компьютера, которые не являются уникальными в глобальном масштабе
32	SECURITY_BUILTIN_DOMAIN_RID — обозначают встроенные идентификаторы SID. Например, известный идентификатор SID для встроенной группы администраторов S-1-5-32-544
80	SECURITY_SERVICE_ID_BASE_RID — обозначают идентификатор SID для служб

Наш идентификатор SID имеет три добавочных подчиненных полномочия: 1534169462, 1651380828 и 111620651. Сами по себе они не имеют никакого самостоятельного значения, но вместе обозначают домен или компьютер, который издал идентификатор SID. Идентификатор безопасности для этого домена — S-1-5-21-1534169462-1651380828-111620651, и все идентификаторы SID будут начинаться с этого набора символов, а заканчиваться каким-нибудь уникальным относительным идентификатором для пользователя или компьютера, который они обозначают. В этом случае идентификатор SID оканчивается на 500, что является общеизвестным относительным идентификатором (RID), обозначающим встроенную учетную запись Administrator (Администратор). 501 — это общеизвестный относительный идентификатор для

встроенной учетной записи Guest (Гость), а 502 — общеизвестный RID для билета на получение билетов (Kerberos Ticket Granting Ticket — krbtgt).

Идентификаторы SID служб

Как упоминалось ранее, службы также имеют идентификаторы SID в Windows Vista и Windows Server 2008. Идентификаторы SID служб всегда начинаются с S-1-5-80 и заканчиваются числом подчиненных полномочий, которое предопределяется именем службы. Это значит, что данная служба имеет один и тот же идентификатор SID на всех компьютерах. Это также значит, что мы можем получить идентификатор SID для произвольной службы, даже если он не существует. Например, чтобы увидеть, какой идентификатор SID мог бы быть у службы foo, запустим команду sc showsid следующим образом:

```
C:\>sc showsid foo
NAME: foo
SERVICE SID: S-1-5-80-2639291829-767035215-3510963033-3734144485-3832470211
```

Если вы попробуете так сделать на одном из ваших серверов, то получите такой же ответ. Если вы предпочли бы иметь более «дружелюбное» имя для службы, используйте NT SERVICE\foo.

Общеизвестные идентификаторы SID

Когда разработчик пишет программу для Windows, ему часто нужно знать идентификатор SID какого-либо принципала безопасности. Обычно идентификаторы SID могут быть легко сконструированы, если известен относительный идентификатор, потому что он просто подставляется к идентификатору SID компьютера или домена, как в случае учетной записи Administrator (Администратор). Однако для удобства часто желательно иметь более краткую и статичную форму некоторых идентификаторов SID. Чтобы это обеспечить, модель безопасности, используемая в Windows, включает значительное количество общеизвестных идентификаторов SID, которые являются одинаковыми на всех компьютерах. Это идентификаторы SID, которые начинаются с S-1-1, S-1-2 или S-1-3, включая некоторые из тех, о которых говорилось ранее в этой главе, такие как CREATOR OWNER SID (S-1-3-0).

В дополнение в Windows NT есть значительное количество общеизвестных идентификаторов SID. Например, S-1-5-32 является общеизвестным идентификатором SID для встроенного домена. Он может, в свою очередь, комбинироваться с общеизвестным относительным идентификатором для формирования общеизвестного SID для конкретной учетной записи. Так, идентификатор SID для встроенной группы Administrators (Администраторы), на домене или на автономном компьютере, всегда S-1-5-32-544. В табл. 1.3 перечисляются некоторые из наиболее часто употребляемых идентификаторов RID, связанных с доменом. В случае встроенных групп связанные с доменом идентификаторы RID могут быть скомбинированы с S-1-5-32 для формирования SID, допустимого на любом компьютере, к которому этот пользователь или группа имеют отношение. Другие учетные группы добавляются к домену, чтобы сформировать полный идентификатор SID. Так, например, происходит с группой Domain Admins (Доменные администраторы), когда берется

общеизвестный идентификатор RID 512 для создания SID, такого, как `S-1-5-21-1534169462-1651380828-111620651-512`.

Таблица 1.3. Общеизвестные относительные идентификаторы, связанные с доменом

RID	Описание
500	Administrator (Администратор)
501	Guest (Гость)
502	Идентификатор RID для билета на получение билетов (Kerberos Ticket Granting Ticket, KRBTGT)
512	Domain Admins (Доменные администраторы)
513	Domain Users (Доменные пользователи)
514	Domain Guests (Доменные гости)
515	Domain Computers (Доменные компьютеры)
516	Domain Controllers (Контроллеры домена)
544	Built-In Administrators (Встроенные администраторы)
545	Built-In Users (Встроенные пользователи)
546	Built-In Guests (Встроенные гости)

Идентификаторы SID могут выглядеть очень запутанными, но, понимая их структуру, их станет довольно легко расшифровывать. Имея даже небольшой опыт, вы сможете легко определить, относится идентификатор SID к службе, общеизвестному принципалу или пользователю в домене. В гл. 3 мы рассмотрим, как эти идентификаторы SID используются для управления правами доступа.

Резюме

Принципалы безопасности и идентификаторы SID лежат в основе столь многого в безопасности Windows, что администраторы должны по крайней мере иметь элементарное представление о том, как они работают. Идентификаторы SID выступают фундаментальными строительными компонентами маркера, который, в свою очередь, является основным инструментом, используемым для проверки права доступа. Понимание того, как эти компоненты функционируют вместе, и умение назначать права, эффективно используя такие инструменты Windows, как пользователи, группы, доменные группы и типы входа, позволят вам работать гораздо продуктивнее и реже сталкиваться с неприятными сюрпризами при более глубоком погружении в безопасность Windows.

Дополнительные ресурсы

- База знаний Microsoft. Поддержка руководств по обеспечению безопасности: статья 885409 (http://support.microsoft.com/?kbid=885409).
- *Libenson E.* Controlling Privileged Accounts to Comply with SOX Section 404 (http://www.s-ox.com/dsp_getFeaturesDetails.cfm?CID=1902).

ГЛАВА 2

Аутентификаторы и протоколы аутентификации

Джеспер М. Джоханссон

Вспомним из гл. 1, что агенты в компьютере называются субъектами, или принципалами безопасности. Когда у вас есть принципал, ему нужен способ доказать, что он на самом деле является тем, за кого себя выдает. Рассмотрим аналогию. Представьте, что вы хотите приобрести что-либо по кредитной карточке в супермаркете, где понимают важность безопасности. Вы прекрасно знаете, что вы — это вы. Однако персонал супермаркета не знает, кто вы, поэтому они требуют некоторое доказательство — аутентификацию, что вы на самом деле тот, за кого себя выдаете. Для предоставления доказательства личности вы используете аутентификатор определенного вида, вроде удостоверения личности или паспорта. Вы предъявляете его клерку в супермаркете, и таким способом осуществляется аутентификация вашей личности. В этом смысле виртуальный мир ничем не отличается от мира реального, за исключением того, что субъект, перед которым вы должны аутентифицироваться, понимает, что подпись на обратной стороне кредитки не является достаточным доказательством для аутентификации. Следовательно, вам нужна более сильная форма аутентификации. В этой главе мы обсудим, какие аутентификаторы поддерживает Windows и как он ими распоряжается.

Типы аутентификаторов

Вообще говоря, есть три типа аутентификаторов:

- то, что вы знаете;
- то, что у вас есть;
- то, кем вы являетесь.

То, что вы знаете

Секрет, который известен вам и во многих случаях также известен системе, в которую вы хотите войти, является простейшей и самой распространенной формой аутентификации: пароль — прекрасный пример того, что вы знаете.

То, что у вас есть

Маркер определенного рода, которым вы владеете, является иным типом аутентификатора. Вы аутентифицируете себя посредством доказательства наличия у вас этого маркера. Примером здесь может служить смарт-карта (ее мы обсудим далее в главе) или одноразовое парольное устройство RSA SecurID (более подробно см. в Интернете на сайте http://www.rsa.com/node.aspx?id=1156). Эти типы знаков почти всегда сочетаются с тем, что вы знаете (пароли и т. д.), и могут серьезно укрепить вашу безопасность.

То, кем вы являетесь

Некоторые системы используют определенную информацию, связанную с пользователем, в качестве аутентификатора. Такие аутентификаторы чаще всего попадают в категорию биометрических — это маркеры, которые измеряют какие-то ваши параметры. Например, сканируют сетчатку глаза, берут отпечатки пальцев или анализ крови, распознают голос. Некоторые специалисты рассматривают ритм печатания в момент набора пароля как биометрический аутентификатор. Использование биометрических аутентификаторов, однако, вызывает споры. В данном случае на самом деле измеряются только параметры того, что вы знаете. Поэтому они могут быть легко захвачены и воспроизведены системой, которая может сделать это без причинения вреда и неудобств субъекту. Следовательно, этот тип аутентификатора не может предоставить двухфакторную аутентификацию.

Вообще говоря, биометрические системы по своей сути неточны. Да, действительно, ДНК представляет точное соответствие, однако очень немногие люди желали бы представлять образцы своей крови только ради того, чтобы воспользоваться компьютером (хотя некоторые компьютеры, которыми я пользовался, казалось, высасывали из меня кровь). Большинство же биометрических факторов не настолько точны, как ДНК. Например, отпечатки пальцев считают уникальными. Но нет уверенности, что многократное их снятие дает абсолютно одинаковые отпечатки, а также что машина может воспроизвести одинаковый результат анализа одного отпечатка дважды. Следовательно, системы биометрической аутентификации в основном оперируют диапазоном приемлемых значений и, когда вы сохраняете свой аутентификатор, вы должны записать его несколько раз. Основываясь на этом, система рассчитывает приемлемый диапазон для вашего аутентификатора. Чтобы успешно пройти аутентификацию, последовательные попытки должны попадать в этот диапазон.

Биометрические системы имеют и множество других недостатков.

Во-первых, за исключением ритма печати, биометрические аутентификаторы требуют специализированных устройств, устанавливаемых для каждого клиента, некоторые из которых могут быть весьма неприятны с точки зрения нарушения вашей личной неприкосновенности. То же верно и для систем, использующих маркеры второго типа, такие, например, как смарт-карты.

Во-вторых, как было сказано ранее, биометрические методы неточны и близкое совпадение — это все, что для них требуется. Для некоторых методов биометриче-

ской аутентификации это может иметь фатальные результаты. Так, если по какой-то причине ваш биометрический аутентификатор изменился, вы не пройдете аутентификацию. Например, при использовании распознавания голоса вы можете не пройти регистрацию, если болезнь или усталость повлияют на ваш голос. Подобным образом злополучный выходной, который вы провели, занимаясь ремонтом дома, может привести к потере цифры, которая вам нужна для входа в компьютер в понедельник утром.

В-третьих, многие считают биометрическую аутентификацию чересчур навязчивой. Необходимость сохранять в компьютерной системе личную информацию, такую, например, как отпечатки пальцев, многим не по душе.

В-четвертых, многие эксперты по безопасности считают достоинства биометрии сильно преувеличенными. Компании, занимающиеся продажей биометрических систем, часто делают не соответствующие действительности утверждения. Например, компания, которая производит программное обеспечение, измеряющее ритм набора, заявляет, что оно защитит клиентов от регистраторов клавиатуры, делая украденные пароли бесполезными. Это не так. Например, пользователь все равно должен набирать пароль на клиентском компьютере и регистратор клавиатуры на клиенте может быть легко модифицирован для регистрации той же информации, что и биометрическое программное обеспечение. Затем эта информация может быть легко воспроизведена для успешной аутентификации. Поэтому использование биометрических аутентификаторов не в состоянии решить в полной мере проблему с паролями. Оно, однако, создает проблему запоминания своих паролей пользователями, потому что в этом случае не подходят варианты, опирающиеся на надежное хранение на клиентской стороне случайным образом генерируемых паролей, таких, например, как Password Safe (более подробно см. в Интернете по адресу http://passwordsafe.sourceforge.net/).

В-пятых, бытует общее заблуждение, что биометрические системы надежны, так как они по своей природе являются частью пользователя и не могут быть оставлены без присмотра, как это может произойти с паролями, записанными, к примеру, на листе бумаги. Однако здесь игнорируется тот факт, что последовательности биометрической аутентификации могут быть не только захвачены, как, например, отпечатки пальцев на стекле, но и сами маркеры вполне возможно изъять. Например, компьютерный клуб Chaos в Германии несколько лет назад опубликовал обучающее видео, показывающее, как получить синтетический отпечаток пальца, сняв его с бутылки. Зафиксированы также случаи, когда воры похищали биометрические аутентификаторы.

И, наконец, в-шестых: выбор биометрических аутентификаторов относительно ограничен. Например, в системе с использованием отпечатков пальцев вам дается только десять вариантов. Если один из них испорчен или потерян, остается девять. Это делает регулярную смену ваших аутентификаторов затруднительной, так как они у вас относительно быстро закончатся. А поскольку захват и воспроизведение доказательств личности представляют серьезный риск, то отсутствие выбора аутентикаторов — это угроза, о которой нельзя забывать.

По всем этим причинам Windows не поддерживает биометрическую аутентификацию.

На рынке существуют компании, которые производят дополнительное программное обеспечение и оборудование для биометрической аутентификации. Microsoft также продает устройство для снятия отпечатков пальцев, хотя оно четко обозначено как устройство безопасности некоммерческого класса. Это объясняется тем, что по причинам, приведенным выше, биометрические аутентификаторы в целом не являются аутентификаторами коммерческого назначения и не должны применяться для защиты важной личной или корпоративной информации. На предприятиях могут быть использованы смарт-карты и пароли, которые будут гораздо более надежными, гибкими и легко интегрируемыми в обычную работу по сравнению с биометрическими маркерами. По этим причинам оставшаяся часть данной главы будет посвящена вопросам применения этих двух аутентификаторов.

Хранение аутентификаторов

Каждый раз, когда у вас есть аутентификатор, вам нужно хранить какую-либо его форму, чтобы при работе его можно было сравнить с тем, что принципал вводит для аутентификации. Метод хранения зависит как от типа аутентификатора, так и от того, как разработчик построил систему.

В этом разделе мы рассмотрим различные способы хранения аутентификаторов в Windows, особенно обращая внимание на пароли, потому что они наиболее часто используются и подвергаются намного большим изменениям, чем смарт-карты.

Смарт-карта зависит от сертификата: она сама содержит секретную часть сертификата (для более подробной информации о сертификатах см. гл. 10). Система аутентификации (в этом случае домен Active Directory) содержит публичную часть. Следовательно, когда мы используем смарт-карты, никакие секреты, относящиеся к смарт-карте, не должны храниться на контроллерах домена. Это в некотором роде упрощает управление смарт-картами по сравнению с паролями.

По соображениям практического характера большинство систем, использующих смарт-карты, отдают секретные ключи в центральное место хранения. В Windows также существует эта возможность. Поступая таким образом, мы можем получить доступ к любым секретам, защищенным смарт-картой, например, для судебных целей. Однако это также значит, что в нашей сети есть важные секреты, нуждающиеся в защите.

Пароли практически в любом исполнении, доступном сегодня, — это секреты, которыми нужно делиться. Секрет, который пользователь применяет, чтобы войти в систему, идентичен тому, который сервер аутентификации применяет, чтобы аутентифицировать доступ пользователя. Это значит, что пароли — это важные секреты и они должны быть защищены. На начальных этапах развития электронно-вычислительной техники в общих компьютерных системах пароли хранились в открытом виде в текстовом файле. Пароли в этих системах никогда не предназначались для ограничения доступа посторонних, в первую очередь потому, что только малая группа людей имела доступ к системе. Они использовались для управления той средой, которую вы получили. В дальнейшем, однако, пароли в парольных файлах были зашифрованы и хэшированы.

Шифрование и хэширование

Шифрование основано на криптографии слов, что в буквальном переводе с английского языка означает «спрятанное письмо». Шифрование — это процесс использования криптографии с целью засекретить написанное, то есть преобразовать что-либо из читабельной формы (обычно именуемой открытым или читаемым текстом) в форму скрытую (называемую зашифрованным текстом). Расшифровка — это операция, обратная шифрованию, которая представляет собой процесс преобразования из зашифрованного текста в открытый.

В то время как шифрование использует криптографию для преобразования чего-либо в нечитабельную, но обратимую форму, хэширование является близким по содержанию процессом, при котором происходит преобразование открытого текста в нечитабельную и необратимую форму. Хэш, например, может быть использован в качестве контрольной суммы для сравнения двух открытых текстов. Если они оба генерируют одинаковый хэш, то у вас есть достаточно оснований считать, что оба открытых текста идентичны. Хэш также обычно меньше (пропорционально открытому тексту), чем зашифрованный текст. Следовательно, хэши очень хорошо подходят для таких целей, как хранение паролей.

Большинство систем на базе UNIX все еще используют именно такую форму хранения паролей с двумя небольшими модификациями.

Во-первых, парольный файл, обычно хранимый в файле `/etc/passwd`, теперь содержит не хэши паролей, а просто имена пользователей и идентификатор. Сами хэши хранятся в теневом парольном файле, например в `/etc/passwd.shadow`. В то время как сам парольный файл открыт для чтения всем, теневой парольный файл могут читать только пользователи, имеющие соответствующие права.

Во-вторых, поскольку хэши паролей изначально были открыты для чтения всем в файле `/etc/passwd`, их необходимо было защищать от атак сравнения. Представим ситуацию, в которой вы и я имеем учетные записи на одном и том же компьютере. Мой пароль — это «pas$word!». И по удивительной случайности вы выбрали тот же пароль. С прямым хэшем мы оба бы имели один и тот же парольный хэш, хранимый в файле `/etc/passwd`. Я бы мог найти мой хэш в файле и затем искать любые другие учетные записи с тем же хэшем. Если бы я нашел хоть один, я бы знал, что у них такой же пароль, как и у меня. Это, безусловно, неприемлемая ситуация. Решением в данном случае будет добавить в пароль перед его хэшированием случайно генерируемые символы — salt («соль»). «Соль» — это просто случайное значение, добавляемое к паролю перед его хэшированием. Оно хранится в открытом текстовом виде в базе данных паролей. Таким образом, даже если два пароля идентичны, они будут иметь разные случайно добавленные символы и, следовательно, разные хэши. Данный процесс показан на рис. 2.1.

Windows использует вариации этих техник для хранения паролей. В следующих разделах мы рассмотрим пять первичных способов хранения паролей в Windows, используемых для аутентификации пользователей самой операционной системой.

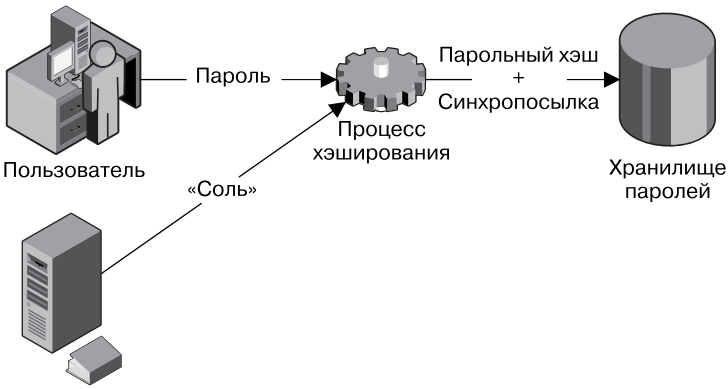

Рис. 2.1. Добавление в пароль перед его сохранением случайных символов позволяет защитить парольный файл от атак сравнения

LM-хэш

LM-хэш — это на самом деле не хэш, хотя и обладает некоторыми его свойствами. LM-хэш — это однонаправленная функция, которая внутри системы обычно называется LMOWF (LanManager One-Way Function). В Windows Vista и Windows Server 2008 LM-хэш во время сетевой аутентификации по умолчанию не хранится и не используется. Однако в ранних версиях Windows LM-хэш обычно и хранится, и передается по умолчанию. Следовательно, знание работы LM-хэша полезно. Заметьте, что и Windows Vista, и Windows Server 2008 могут быть сконфигурированы так, чтобы хранить или аутентифицировать LM-хэш, хотя это и не рекомендуется из-за слабости его алгоритмов.

Прямо из первоисточника: история LM-хэша

LM-хэш впервые был использован корпорацией Microsoft в ее сетевой операционной системе LAN Manager, последняя версия которой была выпущена в начале 1990-х годов. LAN Manager запускалась поверх операционной системы OS/2 IBM. Когда в 1993 году выпускали Windows NT, было правилом, что новая операционная система должна взаимодействовать с LAN Manager. Поэтому организации, инвестировавшие LAN Manager, не сразу обнаружили, что их инвестиции были бесполезны. Однако это также означало, что, хотя Windows NT и поддерживала намного лучшие структуры безопасности, чем LAN Manager, безопасность Windows NT все еще испытывала на себе недостатки конструкторских решений LAN Manager, принятых в середине 1980-х годов. В 2006 году корпорация Microsoft поставила первую операционную систему, которая по умолчанию отключала механизм хэширования паролей LAN Manager, хотя при желании его было можно активировать. Таким образом, понадобилось 13 лет, чтобы отказаться от этой функции.

Джеспер М. Джоханссон, ведущий специалист по безопасности Windows

LM-хэш создается путем выполнения большого количества относительно сложных действий (рис. 2.2). Процесс создания LM-хэша начинается, когда пользователь вводит новый пароль. Этот пароль незамедлительно преобразуется в верхний регистр. Другими словами, пароли, сохраняемые с помощью LM-хэша, не зависят от регистра.

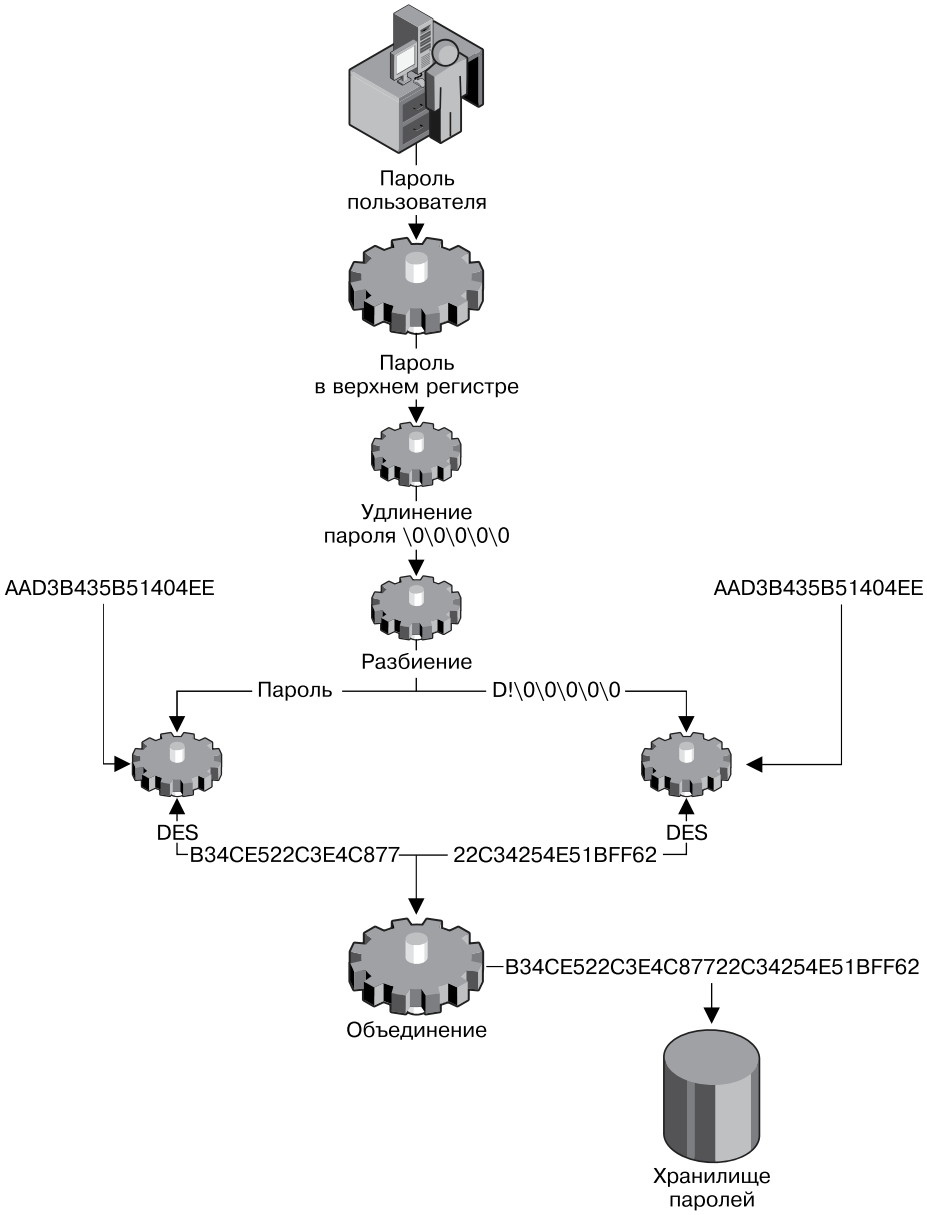

Рис. 2.2. Схема создания LM-хэша

После преобразования в верхний регистр пароль увеличивается до 14 символов. Если пароль длиннее, чем 14 символов, то он теоретически мог бы быть сокращен до этой величины. На практике же, если пароль длиннее 14 символов, LM-хэш не генерируется, а вы получаете предупреждение о совместимости с более старыми операционными системами.

Далее пароль разбивается на две семизначные части. Это делается потому, что теперь они будут использоваться в качестве ключа в шифровании по стандарту шифрования данных (DES), а алгоритм шифрования данных (DEA — алгоритм, применяемый в DES) оперирует с 56-битовыми частями. Эти части используются в качестве ключей для шифрования фиксированного значения.

Наконец результаты двух операций DES объединяются и полученные данные сохраняются в LM-хэше. Хэш сохраняется либо в базе данных диспетчера учетных записей безопасности (SAM) (если пароль является паролем для локальной учетной записи на автономном компьютере или члене домена), либо в атрибуте `DBCS-Pwd` объекта пользователя в службе каталогов Active Directory.

Это объясняет, почему злоумышленник способен определить, какова длина пароля пользователя, просто посмотрев на хэш. Если вторая половина LM-хэша равна `AAD3B435B51404EE`, а вторая половина пароля пуста, то пароль не длиннее семи символов. Если обе половины равны `AAD3B435B51404EE`, то пароль абсолютно пуст.

NT-хэш

Одним из нововведений, представленных в Windows NT, был новый метод хранения паролей. Этот механизм, показанный на рис. 2.3, намного проще, чем механизм создания LM-хэша.

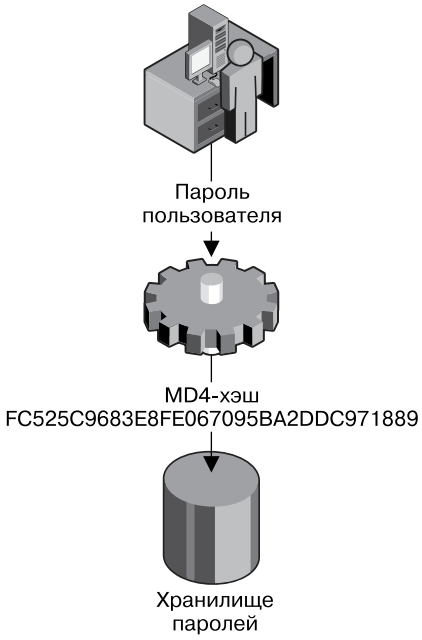

Рис. 2.3. NT-хэш — это простой хэш MD4

NT-хэш, или, как он называется в системе, NTOWF, хранится либо на SAM, либо в атрибуте `Unicode-PWD` пользователя Active Directory.

Заметим, что ни NTOWF, ни LMOWF не используют синхропосылок. Windows никогда не «солила» пароли по той простой причине, что база данных паролей никогда не была доступна для посторонних: чтобы читать базы данных, вам нужно в первую очередь быть администратором, что значило бы, что вы проникли в компьютер или домен. Поэтому проблема «подсматривания» никогда не вызывала особенного интереса в качестве вектора атаки. Более того, системы аутентификации с общим секретом обладают интересным свойством, влияющим на рассматриваемую проблему. О нем мы поговорим далее.

Верификатор пароля

Те, кто работал в среде Windows Active Directory, наверное, замечали, что можно носить с собой ноутбук, соединенный с доменом, и аутентифицироваться в нем с использованием доменной учетной записи, даже не подключаясь к домену. Это «волшебство» происходит благодаря верификатору пароля. Верификатор пароля, часто называемый вне корпорации Microsoft кэшированными учетными данными (cached credentials), является локальной копией доменного парольного хэша. Эту копию мы можем использовать для локального подключения. В версиях операционной системы до Windows Vista верификатор пароля создавался способом, показанным на рис. 2.4.

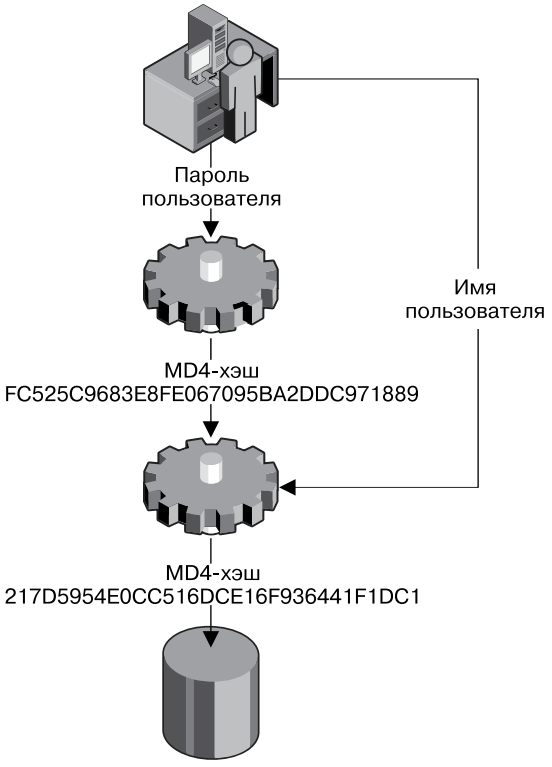

Рис. 2.4. В ранних версиях Windows верификатор пароля был просто хэшем хэша

В последние годы взломщики сосредоточились на верификаторе пароля и начали создавать инструменты для его взлома. Хотя это объединенный с «солью» хэш хэша и, следовательно, его довольно трудно взломать, взлом все-таки возможен, если пароль не очень сложен. Чтобы противостоять этому, в Windows Vista и Windows Server 2008 подсчет верификатора пароля был модифицирован, как это показано на рис. 2.5.

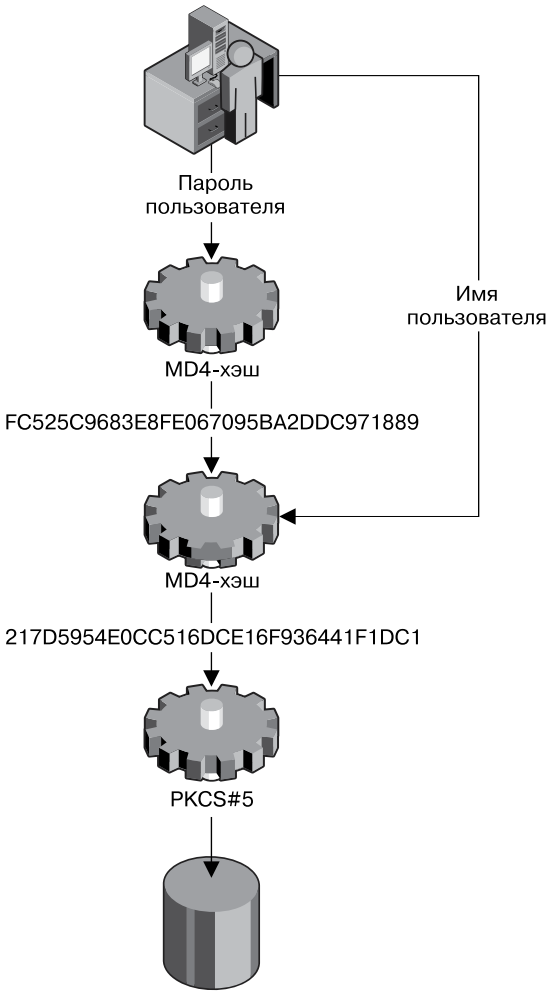

Рис. 2.5. Верификатор пароля в Windows Vista и Windows Server 2008 гораздо сильнее, чем в более ранних версиях

Поскольку нет способа защиты «слабых» паролей, улучшенный подсчет верификатора пароля делает его гораздо надежнее. Пропуская старый верификатор через большое количество операций PKCS #5, взломщик, использующий «грубые» методы, сможет просчитать только около десяти тестов за секунду. Это обеспечивает адекватную защиту для всех паролей, кроме самых простых.

В памяти

Когда пользователь входит в систему, используя терминальные сервисы, Windows кэширует парольный хэш пользователя — NT-хэш и, если компьютер сконфигурирован для его хранения, LM-хэш. Хэш хранится в ячейке памяти, доступной только для операционной системы и, конечно же, для любого процесса, который может вести себя как операционная система. Когда пользователь пытается попасть на сетевой ресурс, требующий аутентификации, операционная система использует этот кэшированный хэш для аутентификации. Это делает возможной «прозрачную» аутентификацию в сетевых ресурсах. Как только пользователь выходит из сети или блокирует рабочую станцию, ячейка памяти автоматически очищается.

Эти хэши превратились в объект сильной критики, после того как было показано, что, если администратор домена вошел в сеть, любой пользователь со статусом администратора может прочитать парольный хэш администратора этого домена и воспользоваться им для аутентификации в контроллере домена (DC) в качестве администратора домена. И хотя это действительно так, для такой атаки требуется слишком много усилий. Если взломщик уже обошел защиту рабочей станции, ему будет гораздо легче установить вспомогательный пакет аутентификации (sub-authentication package), который предоставит пароль в открытом текстовом виде при входе в сеть. Хотя было бы возможно удалить кэшированные парольные хэши, большинство пользователей воспротивились бы необходимости набирать пароль каждый раз при получении доступа к сетевому ресурсу. Если бы эти парольные хэши были убраны, компьютер не мог бы больше «прозрачно» аутентифицировать недоменные сетевые ресурсы для пользователя.

Проблема, следовательно, не в том, как Windows кэширует NT-хэш, и не во вспомогательных пакетах аутентификации, а скорее в образе действий. Доменный администратор никогда не должен интерактивно входить на рабочую станцию, применяемую пользователем с локальными административными правами, если этот пользователь не имеет такого же доверия, как и все доменные администраторы. Следуя такому простому принципу, вы можете охранить эту легальную функцию от атак. Более полную информацию по данному вопросу см. в гл. 13.

Обратимо зашифрованные пароли

Наконец, в Windows есть возможность хранения обратимо зашифрованных паролей. Когда пароль сохраняется обратимо зашифрованным, он может быть переведен в открытый текстовый вид. Очевидно, это означает отсутствие необходимости взлома. Хранение паролей в обратимо зашифрованном виде по умолчанию отключено, и в основном требуется только в двух случаях. Во-первых, оно необходимо, если вам нужно использовать определенные старые протоколы аутентификации для удаленного доступа, такие как CHAP или Digest. Во-вторых, оно требуется, если вы хотите провести углубленный анализ своих паролей после их установки. Например, некоторые организации хотят проанализировать, могут ли пароли содержать определенные слова. Эти организации должны хранить пароли в обратимо зашифрованном виде.

Чтобы активировать обратимое шифрование или проверить, отключено ли оно, используйте Group Policy Management Editor (Редактор объектов групповой политики) (рис. 2.6).

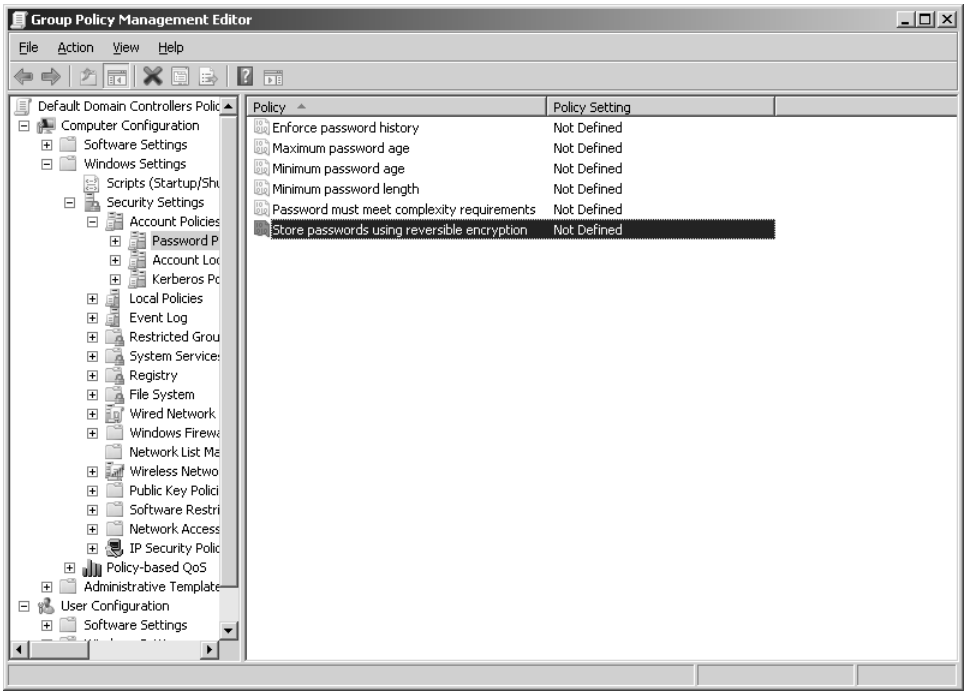

Рис. 2.6. Воспользуйтесь настройками редактора групповых политик, чтобы сконфигурировать компьютер или домен для хранения обратимо зашифрованных паролей

Абсолютное большинство организаций не нуждаются в обратимом шифровании, и, по мере того как клиенты модернизируются и начинают поддерживать более безопасные протоколы аутентификации, остается все меньше и меньше причин его использовать. С другой стороны, обратимое шифрование — это способ хранения паролей в Windows, поэтому важно о нем знать.

Многие морщатся, услышав, что Windows может хранить пароли в обратимо зашифрованном виде. В конце концов, все знают, что хранить пароли в открытом текстовом виде плохо. Однако посмотрим на этот факт с другой стороны. Сегодня в любой системе, использующей пароли, последние эквивалентны открытому тексту. В таких системах используются общие секреты. Единственный же используемый в процессе аутентификации секрет — это тот, который хранится на аутентификационном сервере. Если взломщик захватывает базу данных паролей аутентификационного сервера либо получает доступ к общему секрету каким-либо другим способом, то у него есть все, что требуется для аутентификации. И единственное, что ему нужно сделать, — это внедриться в подходящую стадию процесса аутентификации так, чтобы послать общий секрет пароля, из которого он взят. В настоящее время в Интернете есть несколько бесплатных инструментов, которые производят эти операции с аутентификацией Windows в сети.

Тот факт, что пароли являются эквивалентными открытому тексту, сам по себе не составляет проблемы для безопасности. Он становится проблемой только тогда,

когда взломщик получает парольный хэш. Однако, как вы должны уже понимать, хэши очень хорошо защищены Windows. Если взломщику удается получить парольный хэш, это значит, что он уже подверг риску компьютер настолько же или более, чем ему бы это удалось, взломай он парольный хэш! Другими словами, этот парольный хэш дает ему дополнительные права на уже дискредитированном[1] компьютере.

Если же пароли действительны на других компьютерах, то существует вероятность того, что взломщик может подвергнуть риску и их, используя эти парольные хэши. Более того, поскольку парольные хэши кэшированы в памяти, взломщик может получить доменные административные права с компьютера — члена домена, если доменный администратор находится в сети. Это, однако, главным образом проблема образа действий, относящаяся к тому, как вы управляете своей сетью. Если вы воспользуетесь советами из гл. 11, то сможете адекватно защитить свою систему.

Протоколы аутентификации

До сих пор мы обсуждали, как хранятся пароли в Windows. Теперь поговорим о том, как они используются. Пароли — это аутентификаторы, и, следовательно, их назначение состоит в аутентификации пользователя. Если пользователь интерактивно входит в сеть по локальной учетной записи, то этот процесс достаточно прост.

1. Пользователь использует сочетание клавиш Ctrl+Alt+Delete (SAS, также известное как «комбинация из трех пальцев») для вызова окна входа в систему. Это активизирует локальную подсистему аутентификации пользователей (Local Security Authority Sub-System, LSASS), которая создает новую сессию и загружает процесс WinLogon в этой сессии. WinLogon, в свою очередь, загружает LogonUI.
2. Пользователь набирает свои имя и пароль.
3. Процесс WinLogon принимает пароль, преобразует его в NT-хэш, ищет имя пользователя в локальном SAM и сравнивает NT-хэш с тем, который хранится для данного пользователя. Если они совпадают, то выполняется вход в систему.
4. Если на компьютере установлены вспомогательные пакеты аутентификации, то регистрационная информация передается им для дополнительной обработки. В противном случае запускается файл `user32.exe` и загружается пользовательская среда.

Этот процесс довольно прямолинеен, потому что имеется безопасный канал по всему пути от LogonUI, который принимает открытые текстовые данные, набираемые пользователем, до сравнения этих данных. Но если аутентификация происходит через сеть, она становится немного более сложной, потому что вам приходится беспокоиться о том, как запросы аутентификации передаются между клиентским компьютером, за которым сидит пользователь, и аутентификационным сервером, на котором хранятся базы данных учетных записей. В Windows такая аутентификация может осуществляться в различных формах, которые мы обсудим в следующих разделах.

[1] Дискредитация — несанкционированное раскрытие или потеря защищенной информации.

Базовая аутентификация

Базовая аутентификация относится к самой простой форме аутентификации. В данном случае происходит обычная передача «сырой» регистрационной информации по сети: имя пользователя и пароль посылаются по сети либо в открытом текстовом виде, либо в форме, которая будет передана по сети в неизменном виде, как, например, кодировка Base-64. В некоторых случаях она именуется протоколом аутентификации паролей (Password Authentication Protocol, PAP). Базовая аутентификация довольно распространена в старых сетевых протоколах, таких как Telnet, FTP, POP, IMAP и даже HTTP. Сегодня она может применяться, например, в механизме RPC/HTTPS, предназначенном для соединения клиента Microsoft Office Outlook с сервером Exchange в Интернете. В этом случае данные проходят внутри зашифрованного канала и, в зависимости от того, что заканчивает соединение, передаются либо на сервер Exchange, либо на сервер ISA. Однако, кроме случаев передачи по зашифрованному каналу, следует избегать применения базовой аутентификации.

Запросно-ответные протоколы

Запросно-ответные протоколы предназначены для того, чтобы избежать передачи пароля в виде открытого текста по сети. Все они в основном работают по одинаковой схеме, которая показана на рис. 2.7.

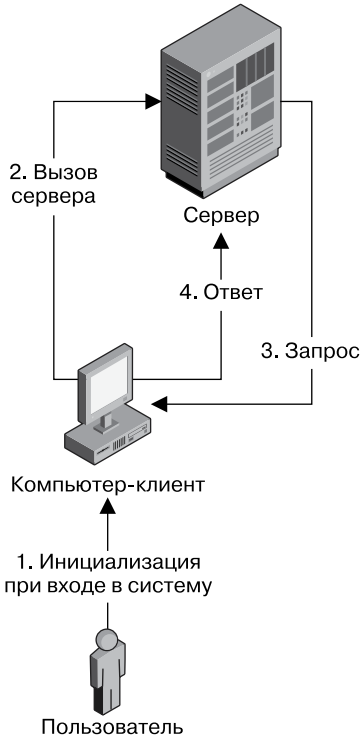

Рис. 2.7. Все запросно-ответные протоколы основаны на одной модели