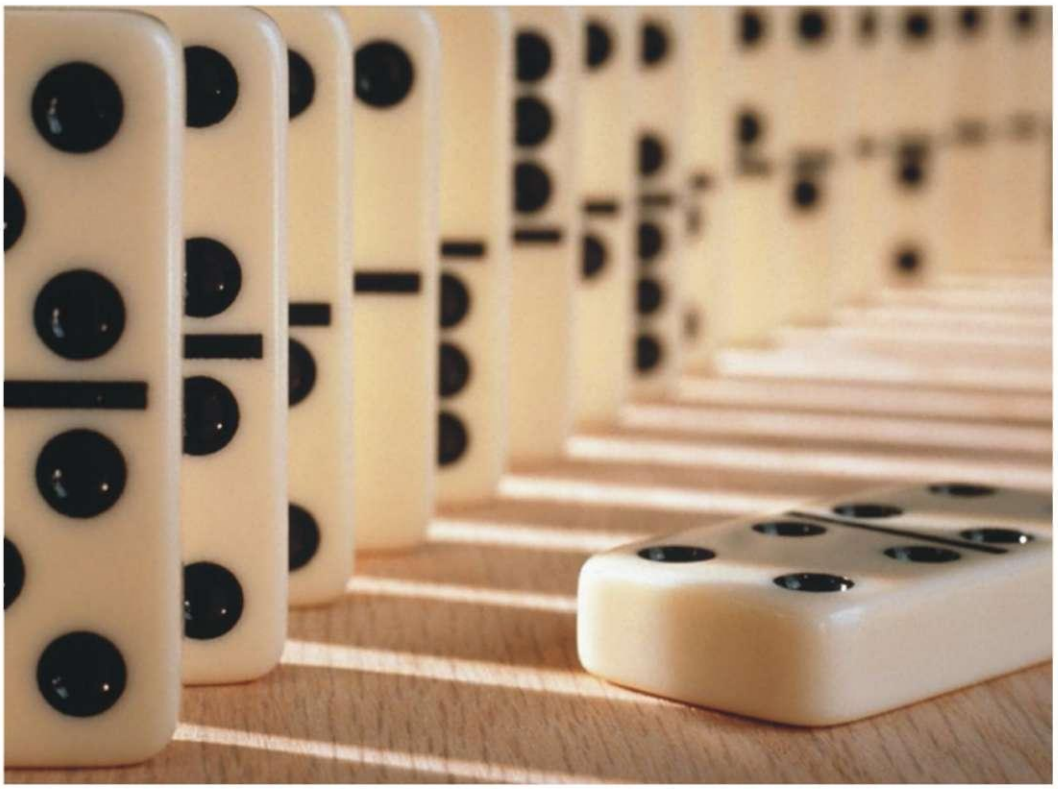
Компания
ИнтерТраст

тел./факс: (495) 956-7928
http://www.intertrust.ru
E-mail: intertrust@inttrust.ru

Е. Киселев



Безопасность IBM Lotus Notes/Domino R7

УДК 821.161.1

ББК 84 (2Рос-Рус) 6-6

К 60

Е. Киселев

«Безопасность IBM Lotus Notes/Domino R7»

В книге рассматриваются вопросы безопасности систем, построенных на базе IBM Lotus Notes/Domino R7. Подробно освещаются процедуры аутентификации и авторизации, шифрование и электронная подпись, сертификаты Notes и X.509, SSL, S/MIME, настройка мониторинга и другие аспекты обеспечения безопасности Notes/Domino. Отдельное внимание уделяется исследованию потенциальных уязвимостей, приводятся рекомендации по их ликвидации.

Книга ориентирована на специалистов по компьютерным сетям, в функции которых входит планирование, настройка и эксплуатация систем на платформе Notes/Domino, а также на менеджеров, отвечающих за корпоративную безопасность компании.

IBM Lotus, IBM Lotus Domino и IBM Lotus Notes являются зарегистрированными торговыми знаками IBM. Все другие упомянутые в данном издании зарегистрированные товарные знаки принадлежат их законным владельцам.

© ИнтерТраст, 2007

© Е. Киселев, 2007

Все права защищены. Никакая часть данной книги не может быть воспроизведена, в какой бы то ни было форме, и каким бы то ни было средствами без письменного разрешения владельцев авторских прав.

ООО «Светотон»
109341, г. Москва, ул. Верхние Поля, д.18
E-mail: svton@from.ru

Подписано в печать 30.07.2007 г. Формат 60x90/8
Печать офсетная. Бумага офсетная № 1.
Усл. печ. л. 45.5. Тираж 500 экз. Заказ

Отпечатано с готового оригинал-макета
в ФГУП «Производственно-издательский комбинат ВИНИТИ»,
140010, г. Люберцы, Московской обл., Октябрьский пр-т, 403.

ISBN 5-7419-0084-4

© InterTrust Co., Tel. +7(495)9567928, http://www.intertrust.ru

Предисловие

Эта книга продолжает серию, начатую Н. Н. Ионцевым – «Системное администрирование *Lotus Domino* для профессионалов». Как он писал в своем предисловии к книге «Почтовая система сервера *Lotus Domino* R5 и ее конфигурирование», продукт *Lotus Domino* достиг того уровня развития, при котором становится очень проблематично подготовить и поддерживать от версии к версии такое учебное пособие, которое охватывало бы все вопросы администрирования, начиная с начального уровня и до степени подробности, требуемой профессионалу.

Выбор темы для этой книги не случаен. Мой опыт работы в учебном центре компании InterTrust говорит о том, что вопросы безопасности являются для слушателей одним из наиболее интересных разделов системного администрирования *Domino*. Система безопасности является основой этого программного продукта, без глубокого понимания которой невозможно стать профессионалом в этой области.

Литературы по *Domino*, а в особенности книг на русском языке, крайне мало. Это особенно удивительно, если учесть количество и масштаб компаний, в которых *Domino* является основой корпоративной информационной системы. Конечно, базовый объем знаний можно получить на авторизованных курсах по системному администрированию. Но мне, при проведении занятий, приходится все время мучиться, когда я пытаюсь затолкать огромный объем информации в жесткие временные рамки. За бортом остается множество подробностей, нюансы, которые могут оказаться крайне полезными в работе.

В результате усилия нашего директора Андрея Линева, все время подталкивавшего меня разродиться хоть чем-нибудь, и мое желание подробно описать хоть какой-то раздел курса принесли свои плоды, и появилась эта книга.

Я не ставил своей целью сделать большой справочник по безопасности *Notes/Domino*. Инструкции типа «для того, чтобы было так-то, нажмите десять кнопок в такой-то последовательности» доступны и без этой книги – например, *Lotus Domino Administrator Help*. Мне было важно показать внутреннюю логику системы, те механизмы, которые спрятаны от поверхностного взгляда.

Книга предназначена для администраторов *Notes/Domino*, имеющих опыт работы в этой области и (или) прослушавших курс по системному администрированию *Domino*. При ее написании предполагалось, что такие базовые понятия, как административный процесс, принцип работы почтовой системы, организация и домен *Domino* хорошо знакомы читателю. Хотя я старался приводить краткий обзор некоторых механизмов, он никак не заменит детального изучения. Подробно описывались только те предметы, которые имеют отношение к основной теме, то есть безопасности.

Структура книги приблизительно соответствует схеме курса «Информационная безопасность сервера *Domino*», но многие разделы дополнены и расширены, а некоторых в курсе просто нет (ну невозможно за три дня детально разобраться с такой обширной темой, как безопасность). Комбинация курс + книга представляется мне оптимальной с точки зрения подготовки профессионального администратора – на занятиях можно уделить основное внимание практической работе, а теоретическая часть излагается в книге.

Особое внимание я старался уделить темам, с которыми у большинства слушателей возникают наиболее серьезные затруднения. В частности, *Internet*-сертификаты, *SSL*, *S/MIME* до сих пор остаются загадкой для большинства администраторов, хотя в последнее время это направление является чуть ли не генеральной линией развития *Notes/Domino*.

Мне бы очень хотелось, чтобы читатель внимательнее отнесся к разделам, посвященным криптографии. Аутентификация, сертификаты и сертификаторы, несимметричное и симметричное шифрование, электронная подпись, сеансовые ключи, *CA*-процесс, центр сертификации и центр регистрации – эти понятия являются фундаментом всей системы. Мало знать, что в *ID*-файле Васи Пупкина есть сертификат. А какого типа сертификат? Как он устроен? Кем заверен публичный ключ, и что значит «заверен»? Как считается хеш, и зачем надо, чтобы он был «соленым»? Будет серьезной ошибкой считать все это излишними подробностями.

У меня были серьезные колебания – а стоит ли рассказывать об уязвимостях *Domino*? После некоторых размышлений я решил, что сделать это просто необходимо. *Domino* –

© InterTrust Co., Tel. +7(495)9567928, http://www.intertrust.ru

замечательный продукт, в нем есть масса средств защиты, но, в отличие от многих других платформ, здесь большинство настроек по умолчанию скорее «разрешающие», чем «запрещающие». Некоторые из них могут привести (и приводят) к очень серьезным неприятностям. Поэтому администратору нужно знать о них заранее. Конечно, можно было написать, как все замечательно, но зачем? Я не рекламный менеджер.

В качестве экспериментальной и демонстрационной платформы использовались версии *Domino* 6.5.3, 6.5.4, 6.5.5, 7.0.1 и 7.0.2. Стендом служили два компьютера – ноутбук и десктоп, оба под управлением *Windows XP SP2*. В книге не рассматриваются особенности функционирования *Domino* на других платформах, за что приношу свои извинения читателям.

Не затронуты также некоторые другие темы. Вообще, книжку оказалось труднее закончить, чем начать – все время всплывали какие-то разделы, про которые тоже надо бы написать. По объему она и так уже получалась раза в три больше, чем планировалась сначала. Поэтому я поступил так же, как поступают с ремонтом, который, как известно, нельзя закончить – можно только прекратить. В результате в этой книге ничего не сказано об интеграции *Domino* с другими продуктами *IBM – DB2, Sametime, QuickPlace, WebSphere Portal*, хотя некоторые аспекты этого взаимодействия напрямую касаются вопросов безопасности. За бортом также остались: смарткарты, работа сервера *Domino* в режиме *ASP* (*Application Service Provider*), поддерживающего несколько «хостируемых» организаций (*xSP*), вопросы сертификации *Domino* в России, продукты сторонних производителей (резервное копирование, антивирусные и антиспамовые пакеты), аппаратные криптографические решения и многое другое. Все это отложено на будущее.

У меня нет никаких сомнений в том, что в этой книге есть куча недостатков и в содержании, и в оформлении. Ошибки тоже наверняка есть. На всякий случай я старался проверять даже самые очевидные для меня вещи, сделав при этом несколько удививших меня открытий. Но вполне мог что-то и прозевать (и, скорее всего, прозевал). Я буду искренне благодарен любым замечаниям, советам, технической информации. Очень интересно было бы получить от читателей описания всяческих тонкостей, хитростей, недокументированных возможностей. Я всегда доступен по почте: *ekiselev@inttrust.ru*, кроме того, все, что вы сочтете нужным, можно высказать в мой адрес на сайте нашего центра обучения: *www.intertrust.ru/education* и в форумс: *www.intertrust.ru/site3/forum.nsf/start?OpenPage*.

Я надеюсь, что переиздания этой книги будут появляться по мере выхода новых версий *Notes/Domino*. В них я постараюсь исправить ошибки и учесть замечания и предложения.

Хочу выразить свою глубокую благодарность **Николаю Николаевичу Ионцеву**, который многому меня научил и чьи книги стали для меня настольными. Это был самый умный и знающий человек в нашем лотусном сообществе. Мне ужасно не хватало его советов и помощи при работе над этой книгой.

© InterTrust Co., Tel. +7(495)9567928, http://www.intertrust.ru

1 *Введение. Модель безопасности Notes/Domino*

Когда книга была уже практически написана, я внезапно обнаружил, что в ней не хватает важной части – введения. Во всех умных книжках оно есть, а в этой – нет. Обычно во введении излагается концепция, подходы, общий взгляд на проблему. Я долго пытался придумать текст, в котором читателю объяснялось, почему безопасность – это хорошо, а ее отсутствие – совсем плохо, что квалифицированный администратор лучше, чем неграмотный, а кругом враги и они не дремлют. Видимо, я не умею писать на такие философские темы. Когда я прочитал то, что получилось, то плюнул и стер.

К счастью, обнаружилось, что эту работу уже проделали ребята из *IBM*. В одной из Красных Книг *IBM* – "*Lotus Security Handbook*" – я нашел подходящую главу, которую перевел, немножко переделал и решил использовать вместо введения. В ней общими словами описывается модель безопасности *Notes/Domino* и кратко излагаются основные понятия. Мне это понравилось, тем более что такой подход вполне согласуется с тем, как я рассказываю об этом на курсах по администрированию: сначала на словах и в самом общем виде, а потом – о том же самом, но уже конкретно, в деталях и с примерами.

Эта глава может оказаться полезной тем, кто совсем недавно знаком с *Notes/Domino*. Профессионалы могут ее спокойно пропустить. Я даже советую им так и поступить.

1.1 *Компоненты модели безопасности Notes/Domino*

Модель безопасности *Notes* базируется на трех основных компонентах: доступ к серверу, доступ к базам, доступ к данным. Данные находятся в базах, базы расположены на сервере. Схематически эта модель изображена на Рис. 1-1.

Рис. 1-1. *Три компонента модели безопасности Notes.*

Мы можем выделить три основных области, которые нам нужно рассмотреть: физическая безопасность, сетевая безопасность и безопасность *Notes*:

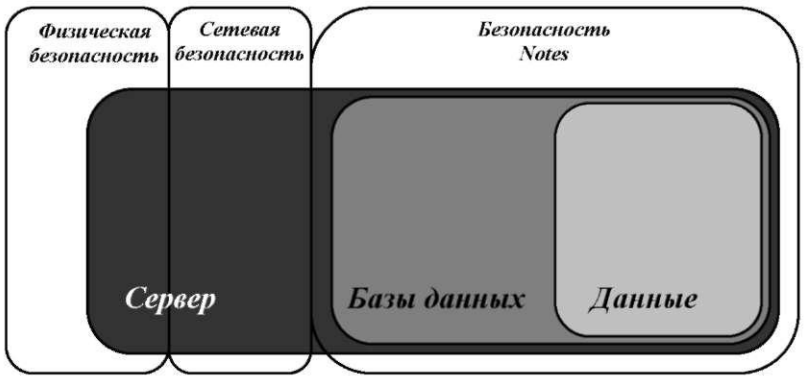


Рис. 1-2. *Три типа проблем безопасности. Под "безопасностью Notes" понимаются встроенные в программный продукт внутренние механизмы безопасности Notes/Domino.*

© InterTrust Co., Tel. +7(495)9567928, http://www.intertrust.ru

Отсюда видно, что, говоря о безопасности сервера, мы должны рассматривать ее с точки зрения физической, сетевой и безопасности *Notes*, в то время как защита баз и хранящихся в них данных рассматривается только с точки зрения безопасности *Notes*. Можно сказать, что общая безопасность модели разделена на две категории: физическая и логическая безопасность. В следующих разделах мы рассмотрим их по отдельности.

1.2 *Физическая безопасность*

Физическая безопасность касается в основном ограничения физического доступа к серверу и хранящейся на нем информации. Она является только одним из аспектов обеспечения общей безопасности сервера, как показано на Рис. 1-3.

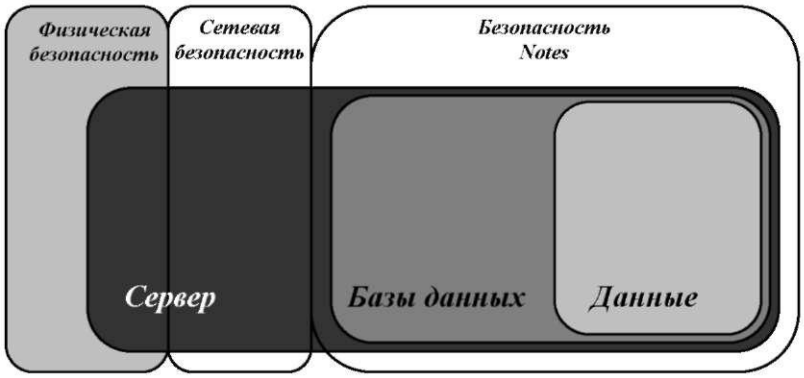


Рис. 1-3. *Физическая безопасность.*

Совершенно ясно, что физическая безопасность сервера должна быть обеспечена. Это предотвратит вмешательство в работу сервера и повреждение, утрату или утечку данных.

Под вмешательством в работу сервера подразумевается доступ к нему неуполномоченных лиц, так же как и любые формы саботажа, влекущие нарушения нормального функционирования сервера.

Повреждение, утрата или утечка данных могут произойти в результате перемещения, изменения или удаления баз.

Ключевые моменты обеспечения физической безопасности заключаются в следующем:

- Сервер должен быть расположен в безопасной зоне, находящейся под охраной и видеонаблюдением.
- Только авторизованный персонал может иметь доступ в серверную комнату. Если сервер находится вне серверной комнаты, то все манипуляции с ним разрешены опять же только авторизованному персоналу.
- У неавторизованных пользователей не должно быть доступа к консоли сервера (***а еще нужно умываться и чистить зубы. Напоминаю, что вся эта глава – перевод. Е.К.***).
- Доступ к серверу для администраторов *Domino* должен осуществляться только с помощью административного клиента *Notes*, *Java-console* или через *Web*-интерфейс базы *Webadmin.nsf*.
- Доступ пользователей к серверу должен осуществляться только через клиент *Notes*, *Web*-интерфейс, или по *Internet*-протоколам, поддерживаемым сервером *Domino, таким как POP3, IMAP, LDAP*. Все прочие способы доступа к данным на сервере (*NetBIOS, Telnet, FTP, NFS*) должны быть запрещены (технически).

© InterTrust Co., Tel. +7(495)9567928, http://www.intertrust.ru

1.3 *Логическая безопасность*

Логическая безопасность касается ограничения сетевого доступа и доступа к данным *Notes*.

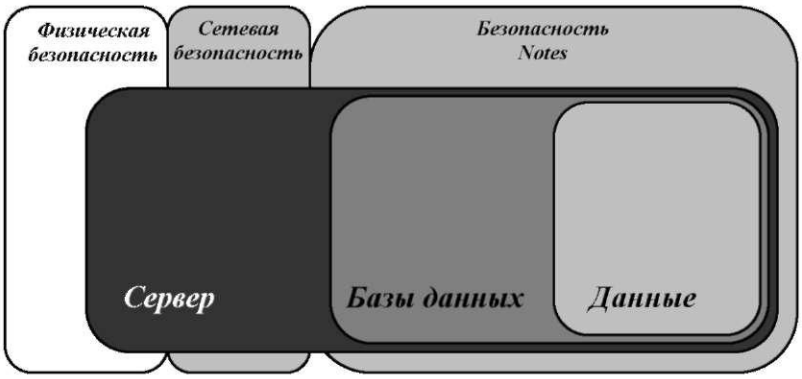


Рис. 1-4. *Логическая безопасность.*

Мы обсудим сетевую безопасность и безопасность *Notes* по отдельности, поскольку в каждой есть своя специфика.

1.3.1 *Сетевая безопасность*

Сетевая безопасность относится к технологиям и оборудованию, которые обеспечивают коммуникацию, то есть передачу данных между устройствами. Это могут быть коммуникации как между серверами, так и между клиентом и сервером. Применительно к *Domino* в качестве клиента может выступать *Notes*, а также различные *Internet*-клиенты: браузер, почтовый клиент, *LDAP*-клиент и т.д. Некоторые архитектуры допускают коммуникацию между клиентами, для *Notes* это невозможно. Клиент *Notes* не может быть «немножко сервером». Область сетевой безопасности, относящаяся к нашей модели, показана на Рис. 1-5.

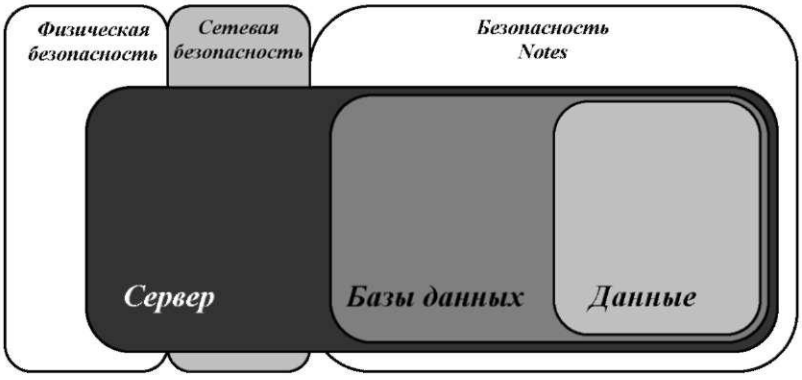


Рис. 1-5. *Сетевая безопасность.*

В следующих секциях описываются элементы сетевой безопасности.

1.3.1.1 Межсетевые экраны

Межсетевой экран (*firewall*) - это устройство контроля доступа в сеть, предназначенное для блокировки всего трафика, за исключением разрешенных данных. Этим оно отличается от маршрутизатора, функцией которого является доставка трафика в пункт назначения в максимально короткие сроки.

Существует мнение, что маршрутизатор также может играть роль межсетевого экрана. Однако между этими устройствами существует одно принципиальное различие: маршрутизатор

© InterTrust Co., Tel. +7(495)9567928, http://www.intertrust.ru

предназначен для быстрой маршрутизации трафика, а не для его блокировки. Межсетевой экран представляет собой средство защиты, которое пропускает определенный трафик из потока данных, а маршрутизатор является сетевым устройством, которое можно настроить на блокировку определенного трафика.

Кроме того, межсетевые экраны, как правило, обладают большим набором настроек. Прохождение трафика на межсетевом экране можно настраивать по службам, IP-адресам отправителя и получателя, по идентификаторам пользователей, запрашивающих службу. Межсетевые экраны позволяют осуществлять централизованное управление безопасностью. В одной конфигурации администратор может настроить разрешенный входящий трафик для всех внутренних систем организации. Это не устраняет потребность в обновлении и настройке систем, но позволяет снизить вероятность неправильного конфигурирования одной или нескольких систем, в результате которого эти системы могут подвергнуться атакам на некорректно настроенную службу.

Существуют два основных типа межсетевых экранов: межсетевые экраны прикладного уровня и межсетевые экраны с пакетной фильтрацией. В их основе лежат различные принципы работы, но при правильной настройке оба типа устройств обеспечивают правильное выполнение функций безопасности, заключающихся в блокировке запрещенного трафика.

Межсетевые экраны прикладного уровня, или прокси-экраны, представляют собой программные пакеты, базирующиеся на операционных системах общего назначения (таких как *Windows* и *Unix*) или на аппаратной платформе межсетевых экранов. Межсетевой экран обладает несколькими интерфейсами, по одному на каждую из сетей, к которым он подключен. Набор правил политики определяет, каким образом трафик передается из одной сети в другую. Если в правиле отсутствует явное разрешение на пропуск трафика, межсетевой экран отклоняет или аннулирует пакеты.

При использовании межсетевого экрана прикладного уровня все соединения проходят через него. Соединение начинается на системе-клиенте и поступает на внутренний интерфейс межсетевого экрана. Межсетевой экран принимает соединение, анализирует содержимое пакета и используемый протокол, и определяет, соответствует ли данный трафик правилам политики безопасности. Если это так, то межсетевой экран инициирует новое соединение между своим внешним интерфейсом и системой-сервером.

Межсетевые экраны прикладного уровня используют модули доступа для входящих подключений. Модуль доступа в межсетевом экране принимает входящее подключение и обрабатывает команды перед отправкой трафика получателю. Таким образом, межсетевой экран защищает системы от атак, выполняемых посредством приложений.

Межсетевые экраны с пакетной фильтрацией могут также быть программными пакетами, базирующимися на операционных системах общего назначения (таких как *Windows* и *Unix*) либо на аппаратных платформах межсетевых экранов. Межсетевой экран имеет несколько интерфейсов, по одному на каждую из сетей, к которым подключен экран. Аналогично межсетевым экранам прикладного уровня, доставка трафика из одной сети в другую определяется набором правил политики. Если правило не разрешает явным образом определенный трафик, то соответствующие пакеты будут отклонены или аннулированы межсетевым экраном.

При использовании межсетевого экрана с пакетной фильтрацией соединения не прерываются на межсетевом экране, а направляются непосредственно к конечной системе. При поступлении пакетов межсетевой экран выясняет, разрешен ли данный пакет правилами политики. Если это так, пакет передается по своему маршруту. В противном случае пакет отклоняется или аннулируется.

Межсетевые экраны с фильтрацией пакетов не используют модули доступа для каждого протокола и поэтому могут использоваться с любым протоколом, работающим через *IP*.

1.3.1.2 Демилитаризованная зона (DMZ)

DMZ – сокращение от "*demilitarized zone*" (демилитаризованная зона). Этот термин используется для обозначения фрагмента локальной сети, не являющегося полностью доверенным. Демилитаризованная зона являет собой область в сети, системы в которой отделены от основной сети. Смысл создания такого сегмента заключается в том, чтобы отделить системы, к которым осуществляют доступ пользователи *Internet*, от систем, с

© InterTrust Co., Tel. +7(495)9567928, http://www.intertrust.ru

которыми работают только сотрудники организации. Демилитаризованные зоны также могут использоваться при работе с партнерами по бизнесу и другими внешними организациями.

DMZ создается посредством реализации полузащищенной сетевой зоны. Данная зона в обычном порядке отделяется сетевыми устройствами, такими как межсетевые экраны или маршрутизаторы со строгими фильтрами. Затем с помощью инструментов управления сетью определяется политика, какому трафику разрешается проникновение в *DMZ*, а какому трафику разрешено выходить за пределы *DMZ*. Как правило, любая система, с которой может установить контакт внешний пользователь, должна находиться в демилитаризованной зоне.

Системы, открытые для прямого доступа внешних систем или пользователей, являются главными целями злоумышленников и потенциально подвержены проявлению угроз. Как следствие, эти системы не могут пользоваться полным доверием. Поэтому необходимо ограничить доступ этих систем к действительно важным и секретным компьютерам, расположенным внутри сети.

Общие правила доступа для *DMZ* позволяют внешним пользователям осуществлять доступ к соответствующим службам на серверах, расположенных в демилитаризованной зоне. На системы в *DMZ* налагаются строгие ограничения на доступ к внутренним системам сети. По возможности соединение между внутренней системой и *DMZ* должно инициироваться внутренней системой. Внутренние системы могут осуществлять доступ к *DMZ* или в *Internet* согласно политикам, однако внешним пользователям доступ к внутренним системам запрещен.

1.3.1.3 Обеспечение сетевой безопасности портов

Функция безопасности портов позволяет настроить какой-либо порт сетевого устройства (как правило, коммутатора) так, чтобы доступ к коммутатору через этот порт предоставлялся только заданному устройству или группе устройств. При обращении к порту с неавторизированного *MAC*-адреса коммутатор может приостановить работу порта или отключить его. Порт может отключаться либо совсем, либо на какое-то определенное время. Возможен также такой режим, когда порт не отключается, а лишь задерживает только те пакеты, которые были отправлены с неавторизованного *MAC*-адреса.

Когда порт получает пакет, *MAC*-адрес отправившего его устройства сравнивается со списком допустимых *MAC*-адресов, который может быть сконфигурирован автоматически или вручную.

Сетевая безопасность порта также может быть сконфигурирована на более высоком уровне – *TCP/IP*. Например, могут быть открыты только *TCP* и *UDP* порты, необходимые для обеспечения функционирования только тех сервисов, которые предоставляет данный сервер.

1.3.2 *Безопасность Notes*

Безопасность *Notes* подразумевает защиту сервера *Domino*, расположенных на нем баз *Notes* и данных, которые содержатся в этих базах (Рис. 1-6).

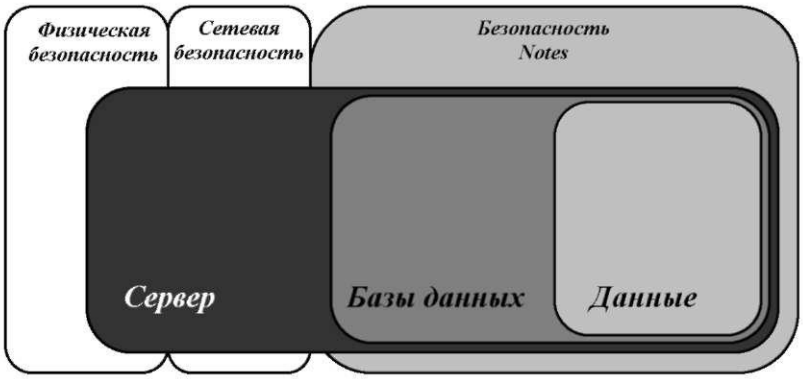


Рис. 1-6. *Безопасность Notes.*

В этой секции описываются элементы безопасности *Notes*.

© InterTrust Co., Tel. +7(495)9567928, http://www.intertrust.ru

1.3.2.1 Сертификация

Notes использует концепцию *ID*-файлов, которая, в свою очередь, базируется на криптографии публичных ключей и сертификатов. Сертификат – это своего рода электронный штамп, который однозначным образом идентифицирует пользователя или сервер. *ID*-файлы пользователя или сервера могут содержать один или более сертификатов *Notes*. Кроме того, в них могут находиться так называемые *Internet*-сертификаты, используемые для идентификации пользователя при установлении *SSL* соединения, а также в электронной подписи и при шифровании *S/MIME* сообщений.

Сертификат содержит:

- имя заверителя, выдавшего сертификат
- имя владельца сертификата (пользователя или сервера)
- публичный ключ, хранящийся как в *ID*-файле, так и в *Domino Directory*. *Notes* использует публичные ключи для шифрования сообщений, посылаемых владельцу публичного ключа, а также для проверки электронной подписи.
- электронную подпись заверителя
- дату истечения срока годности сертификата

Сертификаты хранятся в *ID*-файлах, а также в документах "*Person*", "*Server*" и "*Certifier*" в *Domino Directory*.

Публичные ключи не секретны. Любой пользователь может видеть публичный ключ другого пользователя и применить его для шифрования сообщения или аутентификации. Важно, чтобы каждый, кто видит публичный ключ, был уверен в его надежности. У пользователей должна быть возможность получить публичный ключ заверителя (сертификатора), который выдал этот сертификат, перед тем как аутентифицировать владельца сертификата. Если у пользователя есть сертификат, выданный тем же заверителем, который выдал сертификат другому пользователю или серверу, то он может проверить подлинность их публичных ключей и быть уверенным, что эти ключи связаны с их именами. Если же у них нет общего сертификатора, то для аутентификации потребуется использовать кросс-сертификаты (их еще называют взаимными сертификатами).

Сертификаты *Notes* автоматически создаются для каждого *ID*-файла при регистрации сервера или пользователя. В дополнение к ним в *ID*-файл могут быть добавлены *Internet*-сертификаты. Их может выдать центр сертификации на базе сервера *Domino* или сторонний центр сертификации. *Domino* создает *Internet*-сертификаты в формате *X*.509*v*3, который включает поддержку расширений сертификатов, списков отзыва сертификатов (*CRL*) и точек распространения сертификатов (*CDP*).

1.3.2.2 Шифрование

Криптография – это искусство или наука тайнописи, или, если быть более точным, хранения информации (в течение более или менее длительного времени) в форме, которая позволяет видеть ее только тем, кому вы это разрешили, оставляя ее скрытой для всех остальных. **Криптосистема** – способ выполнения этого. **Криптоанализ** – это практика преодоления попыток скрыть информацию, либо с помощью выявления математических изъянов в криптосистемах (таких, как слабая энтропия), либо с помощью грубой силы – прямым перебором вариантов. **Криптология** включает в себя и криптографию, и криптоанализ.

Исходную информацию, которую требуется зашифровать, принято называть «открытый текст» (*plaintext*, реже *clear text*). Скрытая информация называется «шифрованный текст», или «шифротекст» (*ciphertext*). Процесс конвертирования открытого текста в шифротекст называют шифрованием (*encryption*). Обратную процедуру (превращения шифротекста в открытый текст) называют расшифровкой (*decryption*).

Криптосистемы, такие как та, что встроена в *Notes/Domino*, разработаны таким образом, что расшифровка возможна при соблюдении двух условий. Во-первых, должна быть расшифровывающая программа (например, клиент *Notes* или сервер *Domino* со встроенной

© InterTrust Co., Tel. 7(495)9567928, http://www.intertrust.ru

подсистемой *RSA Security BSAFE Engine*). Во-вторых, необходима некая числовая последовательность, называемая ключом расшифровки, с помощью которой расшифровывающая программа преобразует шифрованный текст в открытый.

Открытый текст преобразуется в шифротекст с помощью шифрующей программы (как правило, одна и та же подсистема занимается и шифрованием, и расшифровкой) и ключа шифрования. Хотя шифрующая программа работает по известному алгоритму и выполняет строго определенную последовательность действий, результат ее работы практически полностью зависит от числовой последовательности, называемой ключом шифрования.

Ключ расшифровки может совпадать, а может и не совпадать с ключом шифрования. Если они совпадают, криптосистема называется «системой с симметричным ключом». Если не совпадают – «системой с несимметричным ключом». Соответственно, ключи шифрования в этих системах носят названия «симметричных» и «несимметричных». В *Notes/Domino* для шифрования используется комбинация обеих систем. Данные шифруются симметричным ключом, а сам этот ключ шифруется публичным ключом получателя и прилагается к данным. Получатель расшифровывает симметричный ключ своим приватным ключом, а затем этим расшифрованным симметричным ключом расшифровывает данные. Такой комбинированный способ шифрования снимает проблему скрытной передачи симметричного ключа получателю.

В *Notes* механизм шифрования/расшифровки данных полностью прозрачен для пользователя. При наличии у него необходимого для расшифровки ключа, данные расшифровываются автоматически.

1.3.2.3 Электронная цифровая подпись

Электронная цифровая подпись (ЭЦП) основана на шифровании, но предлагает другую форму электронной безопасности. Она заверяет получателя подписанного с помощью ЭЦП сообщения в том, что оно было послано именно тем лицом, кто его подписал, и с момента подписания его содержание осталось неизмененным. То же самое относится и к подписанному документу, хранящемуся в базе – ЭЦП означает, что документ является подлинным и его содержимое не искажено кем-либо посторонним. Кроме того, электронная подпись гарантирует, что подписавший этот документ (как правило, это его автор) не сможет утверждать, что он не посылал этого сообщения (или не создавал этот документ). Это называется «безотзывность» (*non-repudiation*).

Так же как и шифрование, механизм электронной подписи совершенно прозрачен для пользователя. И подписание, и проверка ЭЦП происходят автоматически. Электронная подпись (к примеру, для почты) действует следующим образом:

1. Почтовый клиент отправителя вычисляет дайджест сообщения. Дайджестом здесь называется результат хеш-преобразования исходного сообщения, которое из содержимого письма вычисляет числовую последовательность фиксированной длины, однозначно соответствующую исходному сообщению.
2. Почтовый клиент отправителя шифрует этот дайджест приватным ключом пользователя. Затем к письму присоединяются этот шифрованный дайджест и сертификат отправителя, содержащий его публичный ключ.
3. Почтовый клиент получателя расшифровывает дайджест сообщения, используя публичный ключ отправителя, извлеченный из его сертификата.
4. Почтовый клиент получателя вычисляет дайджест сообщения, а затем сравнивает его с тем, который был извлечен из электронной подписи и расшифрован. Если они идентичны, это означает, что сообщение действительно было послано этим отправителем и не было изменено по дороге.

1.3.2.4 Контроль доступа

Каждая база данных имеет список контроля доступа (*Access Control List, ACL*), который сервер *Domino* использует для определения уровня полномочий пользователей и других серверов по отношению к этой базе.

Когда пользователь открывает базу, сервер *Domino* определяет, какой уровень доступа назначен для него в *ACL*, и предоставляет полномочия в соответствии с этим уровнем. В разных базах у пользователя может быть разный уровень доступа.

Уровень доступа, присвоенный пользователю, определяет, какие операции он может производить в этой базе. Для сервера этот уровень определяет, какая информация ему доступна при репликации. Изменять *ACL* базы, расположенной на сервере, может только тот, кто имеет уровень доступа *Manager*.

Снизу вверх эти уровни можно расставить так: *No Access, Depositor, Reader, Author, Editor, Designer, Manager.*

1.3.2.5 Контроль исполнения

Список доступа на исполнение (*Execution Control List, ECL*) дает возможность пользователям защитить свои данные от таких угроз как почтовые бомбы, вирусы, трояны и другого вредоносного кода. *ECL* предоставляет механизм управления тем, какие программы разрешено выполнять, и какой уровень допуска будет им предоставлен. Он настраивается на уровне отдельных пользователей, причем весьма детально. Например, пользователь может предусмотреть, что в документах, подписанных его коллегами (которым он доверяет), может содержаться исполняемый программный код. Этому коду разрешен доступ к документам и другим базам, но запрещен запуск внешних программ и доступ к файловой системе.

Для проверки исполняемого кода *ECL* использует электронную подпись. Когда производится попытка исполнения этого кода, *Notes* проверяет, кем этот код подписан, а затем обращается к *ECL* с тем, чтобы определить, какое действие можно разрешить автоматически, а о чем нужно спросить пользователя. Если имя того, кто подписал этот код, найдено в *ECL* – явно, в виде иерархического шаблона (**/Lotus)*, или по умолчанию (*-Default-*) – и соответствующее действие разрешено, то оно выполняется автоматически. Если имя подписавшего код не найдено, либо найдено, но требуемое действие не разрешено, то *Notes* в диалоговом окне предлагает пользователю принять решение, как в этой ситуации поступить. Предлагаются такие варианты:

- не выполнять
- выполнить один раз
- доверять подписавшему на время этой сессии
- доверять подписавшему

Если код вообще не подписан, то правила его выполнения определяются записью *"No Signature"* в *ECL*.

1.3.2.6 Локальная безопасность

Понятие «локальной безопасности» (*local security*) относится к возможности шифрования всей базы целиком с помощью публичного ключа сервера или пользователя. База, расположенная на сервере, может быть зашифрована только с помощью публичного ключа данного сервера. Локальную базу можно зашифровать публичным ключом любого пользователя.

Локальное шифрование защищает базу от тех, кто каким-либо образом получил доступ к файлу этой базы, но не имеет соответствующего приватного ключа для расшифровки. Это увеличивает безопасность, так как для того, чтобы получить доступ к данным, требуется иметь не только базу, но и *ID*-файл с необходимым ключом, а также знать пароль, которым защищен этот *ID*-файл.

ID-файл пользователя необходим для доступа к зашифрованной базе, расположенной на клиенте *Notes*. Если же база находится на сервере, и зашифрована его публичным ключом, то для тех пользователей, которые будут к ней обращаться через сервер, он будет расшифровывать ее с помощью своего *Server.id*.

Конец вводной части. Перевод закончен, дальше уже мой текст.

© InterTrust Co., Tel. · 7(495)9567928, http://www.intertrust.ru