Федотов А.М. Информационная безопасность в корпоративной сети // Проблемы безопасности и чрезвычайных ситуаций / ВИНИТИ. - М.: ВИНИТИ, 2008. - N 2. - С.88-101

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КОРПОРАТИВНОЙ СЕТИ*

член-корреспондент РАН А.М.Федотов
(НГУ, ИВТ СО РАН)

В данной работе сделана попытка обсудить основные проблемы, связанные информационной безопасностью в корпоративной сети и обеспечением надежного функционирования информационных систем и предоставляемых ими услуг. Под информационной безопасностью понимается защищенность информационных ресурсов (информационных систем) и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информационных ресурсов

Введение

Проблема доступа к информационным (в том числе и к вычислительным) ресурсам является одной из основных проблем, возникающих в деятельности научного сообщества. В настоящее время наблюдаются переход к распределенной схеме создания и поддержания информационных ресурсов и, в то же время, – стремление к виртуальному единству посредством предоставления свободного доступа к любым ресурсам в сети через ограниченное число «точек доступа». Особенно остро эти проблемы стоят в Сибирском отделении РАН, в связи с его значительной территориальной распределенностью.

Сибирское отделение РАН является региональным объединением научно-исследовательских, опытно-конструкторских, производственных организаций и институтов, а также подразделений, обеспечивающих функционирование инфраструктуры научных центров, расположенных на территории Сибири в 7 областях, 2 краях и 4 республиках (общая площадь территории около 10 миллионов км^2). Научные центры Отделения находятся в Новосибирске, Томске, Красноярске, Иркутске, Якутске, Улан-Удэ, Кемерово, Тюмени, Омске, отдельные институты работают в Барнауле, Чите, Кызыле. В составе СО РАН порядка 100 научно-исследовательских и конструкторско-технологических институтов, работающих в области физико-математических, технических, химических и биологических наук, наук о Земле, гуманитарных и экономических наук. Примерно половина научного потенциала Отделения сосредоточена в Новосибирском научном центре СО РАН [1].

Осознание необходимости интеграции разнородных научных ресурсов (информационных и вычислительных) привело к созданию интегрированных (единых) *научных информационных систем*, которые позволили бы установить связи между разнородными ресурсами и документами, организовывать единые каталоги документов, создавать специализированные системы поиска, а также соблюдать единые правила доступа к этим ресурсам. Необходимы новые концепции, способные обеспечить доступ к приложениям и совместное использование распределенных ресурсов, поддерживающие общую логику доступа, обеспечения информационной безопасности, эффективное управление распределенными ресурсами, а также выявление проблем и других ключевых параметров качества обслуживания.

По-видимому, единственный путь к решению этой проблемы состоит в интеграции в рамках интегрированной распределенной информационной системы данных локальных информационно-справочных систем, существующих в Институтах, и придания этим системам функций глобальной (корпоративной) аутентификации и авторизации пользователей по доступу к информационным ресурсам. Очевидно, что проблемы доступа к

* Работа выполнена при частичной поддержке РФФИ: проекты 06-07-89060, 06-07-89038, 07-07-00271, президентской программы “Ведущие научные школы РФ” (грант № НШ-9886.2006.9) и интеграционных проектов СО РАН.

информационно-вычислительным ресурсам не могут быть решены в рамках только централизованных корпоративных информационных систем, особенно для корпораций, охватывающих значительную территорию, каким является Сибирское отделение РАН.

Корпоративные информационно-телекоммуникационные системы предназначены для получения определенных информационных услуг. Если по тем или иным причинам получение этих услуг пользователями становится невозможным, это наносит ущерб всем субъектам информационных отношений. В контексте данной работы *система информационной безопасности в корпоративной сети* понимается как совокупность организационных мер и технологических решений для обеспечения *доступности, целостности (актуальности и непротиворечивости информации, ее защищенность от разрушения и несанкционированного изменения) и конфиденциальности (защита от несанкционированного доступа).*

Исходя из этого тезиса можно сформулировать основные задачи обеспечения информационной безопасности как:

- создание механизмов своевременного выявления, прогнозирования, локализации и оперативного реагирования на угрозы безопасности и проявления негативных тенденций в использовании информационных ресурсов и систем;
- создание эффективных регламентирующих документов обеспечения информационной безопасности;
- создание технологической и материально-технической базы информационной безопасности;
- обеспечение правовой защиты субъектов информационных отношений;
- сохранение и эффективное использование информационных ресурсов;
- координация деятельности субъектов информационного обмена в обеспечении информационной безопасности;
- унификация требований к обеспечению информационной безопасности;
- обеспечение надежного функционирования информационных систем и предоставляемых ими услуг.

Отметим, что проблемы информационной безопасности затрагивают все уровни научно-технологического обеспечения — от теоретических основ и международных стандартов до оперативного администрирования.

Следует отметить ряд проблем, связанных с подходами к созданию и развитию информационных систем, которые непосредственно связаны с задачами информационной безопасности, но им не всегда уделяется должное внимание. Наиболее серьезные из них следующие:

- Отсутствие оценок перспектив развития системы, в результате чего у системы не остается возможностей для количественного либо качественного роста. При внедрении средств информационной безопасности это может привести к существенной перестройке системы практически сразу же после ее построения.
- Привязка к жестко определенной инфраструктуре обуславливается обычно стремлением использовать известные или применяющиеся ранее технологии, что при необходимости перехода на другие технологии систему невозможно динамично модернизировать в обозримые сроки и без значительных затрат.
- Если система строится в расчете на определенные инфраструктурные решения, то часто бывает невозможно разделить инфраструктурные и прикладные компоненты системы. В результате создания защищенной инфраструктуры зачастую информация, обрабатываемая в прикладных системах, остается незащищенной.

Следует также отметить, что основная угроза информационной безопасности организаций как это ни странно исходит не от внешних источников, а от *собственных сотрудников*.

Федотов А.М. Информационная безопасность в корпоративной сети // Проблемы безопасности и чрезвычайных ситуаций / ВИНИТИ. - М.: ВИНИТИ, 2008. - N 2. - С.88-101

Особенности больших корпоративных сетей

Существующие в настоящий момент большие корпоративные сети, как например СПД (сеть передачи данных) СО РАН, возникли не сразу, а развивались в течении многих десятилетний. Например, работы по созданию СПД СО РАН были начаты в далеких 70-х годах прошлого столетия. За прошедшие годы несколько раз менялись поколения вычислительной техники и технологий связи. Как это ни странно, основной проблемой больших корпоративных сетей является их размер. Наличие сложных сетевых конфигураций в совокупности с требованиями к безопасности и надежности функционирования сервисов – в больших системах приводит к проблемах, которые начинают принимать глобальные масштабы.

За годы своего существования СПД СО РАН по числу пользователей и компьютеров, по объемам передаваемых данных, по количеству и качеству накопленных информационных ресурсов, по разнообразию и качеству предоставляемых услуг превратилась в крупнейшую корпоративную научно-образовательную сеть России. В СПД СО РАН зарегистрировано около 150 организаций-абонентов. Только в Новосибирске сеть обслуживает более 40,000 пользователей и насчитывает более 12,000 подключенных компьютеров. Кроме того, в региональных научных центрах Отделения находится еще около 30,000 пользователей. Все работы по эксплуатации и развитию СПД СО РАН реализуются в рамках корпоративного подхода [2].

Характерной особенностью больших сетей, таких как СПД СО РАН, является использование наличие большого числа разнообразных аппаратно-технических средств. Они различаются своими характеристиками, производительностью, аппаратными платформам и базовыми технологиям. Подобное разнообразие объясняется несколькими причинами: аппаратура приобреталась в разное время; ее подключение производилось разными специалистами, использовавшими разные технологии построения информационной сети; развивалась и топология сети путем присоединения корпоративных сетей региональных научных центров. Указанные обстоятельства породили ряд серьезных проблем для обеспечения информационной совместимости и безопасности систем.

Рассмотрим основные особенности больших сетей, которые необходимо учитывать при анализе проблем информационной безопасности:

Сложные сетевые конфигурации. Большая сеть неизбежно имеет достаточно сложную и не всегда ясную структуру. Получить «правильную» карту сети с указанием всех существующих сегментов, а также планов развития сетевой инфраструктуры, зачастую является неразрешимой проблемой. Однако, для обеспечения информационной безопасности сети необходима достоверная информация по различным аспектам — адресация, маршрутизация, физические соединения, информационные потоки, статистика по загрузке и другие показатели. Как правило, не составляет трудностей получение подобной информации по какому-либо конкретному сегменту системы, составление же общей картины оказывается достаточно сложной задачей.

Различные скорости связи. Серьезные проблемы при построении интегрированных систем безопасности возникают в связи с различием скоростей передачи данных на разных участках информационных систем. Как правило, эти каналы строились без анализа требований по обмену данными, что вызывает дополнительные трудности, связанные с обеспечением качества обслуживания.

Большой парк разнообразного оборудования. Характерной особенностью больших корпоративных сетей является наличие огромного количества аппаратно-технических средств. Они различаются не только по производителю и характеристикам, но и по платформам и технологиям. Аппаратура приобреталась в разное время; закупки и внедрение производились разными специалистами, которые не только имели свои предпочтения, но и по-разному представляли структуру информационной сети. Это является серьезной проблемой для построения системы информационной безопасности.

Гетерогенные системы. Большая корпоративная сеть является, как правило, объединением сетей более мелких (как в случае СПД СО РАН, сетей организаций-участников сети). По этой причине возникает целый ряд специфических проблем, связанных с совместимостью различных платформ, версий ОС, версий прикладного программного обеспечения и т.п. и используемых технологий в этих организациях. Это приводит к необходимости разработки решений по интеграции этих технологий. Например, применение для авторизации различных вариантов туннелирования вызывает проблемы с совместимостью устройств. Сейчас программное обеспечение разрабатывается с очень коротким жизненным циклом, а современные угрозы требуют постоянного ответа на уязвимости. Быстрое обновление поколений продуктов в сочетании с размерами сети и требованиями по производительности и надежности приводят к необходимости последовательного обновления программного и аппаратного обеспечения. Учитывая, что в большой сети не всегда можно произвести полномасштабное обновление за короткий период времени, определяются требования к совместимости продуктов между собой. Обеспечение таких возможностей требует значительных усилий по *моделированию* ситуаций, отработке надежных сценариев миграции и высокой квалификации специалистов.

Недостаток контроля. При запуске оборудования или программного обеспечения от них в первую очередь требуется выполнение основной функции. Все остальные функции могут быть оставлены на потом или не использованы вообще. Системы журналирования, оповещения, удаленного управления и *безопасности* страдают от такого отношения к делу. Кроме того, из-за растянутости во времени процесса развития сети с привлечением разных специалистов возникают ситуации, когда у владельца сети теряется или радикально меняется понимание логики организации отдельных ее элементов. Возникают, так называемые, «медвежьи углы», о которых никто из сотрудников не имеет представления. В результате процесс внедрения любой системы приводит к необходимости всестороннего исследования инфраструктуры и информационных потоков, не гарантируя при этом стопроцентного отсутствия проблем. Минимизировать эту проблему позволяет планирование и документирование сетевой инфраструктуры. Наличие подробного плана сети с документально закрепленными зонами ответственности, с документированной и согласованной стратегией развития является редкостью, но без этого практически любое серьезное вмешательство в инфраструктуру (а внедрение любого вида средств безопасности в работающую сеть является таким вмешательством) может привести к большому количеству проблем.

Размывание зон ответственности. К сожалению, в больших и распределенных информационных сетях происходит размывание зон ответственности. Во-первых, разные части сети находятся в разном административном подчинении и могут развиваться без учета «общей картины мира». Во-вторых, в больших сетях каждый администратор, как правило, знает только свою часть сети, в то время как пограничные участки, лежащие на стыках, им неизвестны. Это приводит к возникновению «белых пятен» на карте информационной сети, а значит, к серьезным уязвимостям в информационной безопасности.

Отсутствие «общей картины мира». Получить «общую картину мира» из одного источника в больших сетях практически невозможно. Разные зоны ответственности, отсутствие сформулированной в документах и руководствах идеологии построения и развития системы приводят к тому, что нет общего понимания происходящего. При попытке работать на стыке нескольких зон ответственности, как обычно бывает со средствами безопасности, возникают характерные проблемы, основной из которых является неопределенность последствий.

Географическая распределенность. Как правило, большая корпоративная сеть являются географически распределенной системой. Для взаимодействия и обмена данными в таких системах применяются различные каналы от «доступа в Интернет» до собственных или арендованных. Это приводит к необходимости держать большой штат инженеров для

реагирования на проблемы, требует изрядных ресурсов на внедрение и обеспечения оборудованием и комплектующими. Географическая удаленность различных объектов инфраструктуры больших сетей автоматически тянет за собой проблему распределения по часовым поясам. Разница во времени приводит к сложностям в координации усилий по согласованному переключению оборудования.

Неполное функционирование системы в каждый конкретный момент. Из-за большого количества аппаратно-технических средств, распределенных географически, возникает вероятность того, что часть оборудования, в том числе системы безопасности, может не функционировать в определенный момент времени. К примеру, при загрузке политики на устройства централизованно из единого центра управления существует необходимость в установлении устойчивой связи со всеми удаленными площадками и объектами. Если хоть один из каналов связи будет блокирован, данная операция может привести к разного рода проблемам. Система управления должна уметь определить такую ситуацию, исправить ее или иным образом, чтобы обеспечить выполнение поставленной задачи. Масштаб проводимых работ практически исключают одновременность событий, поэтому модернизация должна осуществляться путем серии последовательных изменений.

Основные требования к инфраструктуре управления

Современные крупные распределенные системы, с учетом условий их эксплуатации, а также постоянно возникающих проблем их функционирования предъявляют серьезные требования к обеспечению безопасности. Во-первых, эти системы должны «выдерживать» радикальные изменения направлений развития. Во-вторых, они должны быть достаточно гибкими и допускать контроль своего поведения в сложных условиях эксплуатации. Даже если произойдет смена концепции информационной системы (что бывает нередко), комплекс информационной безопасности должен работать надежно и без сбоев и выполнять свою основную задачу [3].

Требования к гибкости. В корпоративных сетях со сложной конфигурацией значительно повышаются требования, предъявляемые к гибкости продуктов безопасности и систем управления. Даже очень хорошо работающая система информационной безопасности (даже коммерческая) может не иметь достаточных конфигурационных возможностей. К сожалению, многие продукты не обладают необходимой гибкостью и не могут без проблем интегрироваться в сети со сложной конфигурацией.

Неизбежность последовательных изменений. Отличительной особенностью больших систем является то, что невозможно производить какие-либо изменения и модернизации, отключив при этом всю сеть. При проведении работ по модернизации или обслуживанию систем безопасности, тем самым, не избежать последовательных изменений. Любые изменения должны производиться поочередно в отдельных сегментах сети, продвигаясь шаг за шагом, с учетом, описанных выше сложностей. Идея полного отключения информационной системы вряд ли найдет поклонников среди пользователей информационных ресурсов. Кроме того, плановые последовательные изменения являются необходимым требованием *распределения зон ответственности*.

Распределение зон ответственности. Размывание зон ответственности в больших сетях приводит к необходимости обеспечения высокой степени координации управления системами безопасности и сегментами большой сети, находящимися в различных частях. При этом мы всегда имеем ограниченное количество ресурсов управления и специалистов. Учитывая то, что за отдельные участки системы отвечают различные люди, необходимо четко планировать и *распределять* ответственность при внедрении и управлении средствами информационной безопасности в больших сетях.

Возможность отката изменений. Всегда при выполнении изменений существует вероятность, что новое состояние будет хуже прежнего. Виной этому могут быть: ошибки, проявившиеся в данной конфигурации, неучтенные особенности, человеческий фактор,

повышенные требования к производительности платформы у новой версии и т.д. Поэтому необходимо планировать варианты отката изменений, собирать и обобщать опыт во избежание подобного в будущем.

Надежность системы. В больших сетях, как, впрочем, и в любых других, всегда предъявляются очень высокие требования к надежности функционирования системы и доступности данных. Это ограничивает действия по управлению средствами и системами безопасности. Часто нет возможности, например, остановить функционирование системы серверов, чтобы провести профилактическую работу. И наоборот, если происходит остановка какого-то сегмента сети, то система безопасности должна быть готова к таким событиям. Обеспечение систем управления безопасностью, связанное с сервером по этому каналу, должно уметь обрабатывать случаи, когда пропадает связь на каком-либо транзитном участке. При работе в распределенном сетевом окружении всегда надо учитывать потенциальную вероятность отказов оборудования и принимать меры к минимизации их влияния.

Переходные ситуации. Надежность системы подразумевает, помимо всего прочего, готовность системы безопасности к возможной переходной ситуации, когда изменения в инфраструктуре произведены еще не полностью. При этом функционирование организации и безопасность информационной инфраструктуры должны обеспечиваться беспрерывно, вне зависимости от того, закончены работы или нет.

Отказ в обслуживании. Когда мы говорим о надежности и доступности, мы также должны учитывать возможные ситуации, когда система безопасности не может по каким-то причинам выполнить поставленные перед ней задачи. В этом случае система должна их четко определять, а сами действия осуществлять либо позже, либо обоснованно отвергать их выполнение, поскольку на текущий момент система к этому не готова.

Ограниченные ресурсы Немаловажное требование: обслуживание систем должно выполняться ограниченными ресурсами по времени и численности персонала. Хорошо спланированная и реализованная, подкрепленная документацией система не требует для эксплуатации большого количества сотрудников, но предъявляет высокие требования к качеству обслуживания.

Стандарты информационной безопасности

В области информационной безопасности в настоящий момент действует большое число стандартов, взаимодополняющих друг друга, как международных, так и отечественных. Наиболее важными из них являются рекомендации[1] серии X рабочей группы № 17 международного телекоммуникационного союза (ITU-T). Не останавливаясь подробно на их описании, приведем основные рекомендации по обеспечению информационной безопасности.

Рекомендации этой серии описывают основы информационной безопасности в привязке к эталонной семиуровневой модели ISO/OSI. Эти рекомендации предусматривают администрирование средств безопасности и следующие сервисы безопасности:

- **Аутентификация.** Имеются в виду: аутентификация партнеров по общению и аутентификация источника данных.
- **Управление доступом**. Обеспечение защиты от несанкционированного использования ресурсов.
- **Конфиденциальность данных.** Предусматривается как защита, так и защита трафика.
- **Целостность данных.** Данный сервис подразделяется на подвиды в зависимости от того, что контролируется — целостность сообщений или потока данных, обеспечивается ли восстановление в случае нарушения целостности.

1 Большая часть которых стандартизована Международной организацией по стандартизации – ISO.

- **Неотказуемость.** Данный сервис относится к прикладному уровню, то есть имеется в виду невозможность отказаться от содержательных действий.

Администрирование средств безопасности включает в себя передачу информации, необходимой для работы сервисов безопасности, а также сбор и анализ данных об их функционировании. Основой администрирования является информационная база управления безопасностью. Эта база может не существовать как единое (распределенное) хранилище, но каждый компонент системы должен располагать информацией, достаточной для проведения в жизнь политики безопасности. Отметим, что в корпоративной сети администрирование перестает быть внутренним делом организации. Во-первых, плохо защищенная система может стать плацдармом для подготовки и проведения злоумышленных действий. Во-вторых, прослеживание нарушителя эффективно лишь при согласованных действиях многих администраторов.

Сервисы безопасности, какими бы мощными они ни были, сами по себе не могут гарантировать надежность программно-технического уровня защиты. В этом отношении важнейшим является *архитектурный принцип* невозможности обхода защитных средств. Только правильно спланированные архитектурных решения могут сделать эффективным объединение сервисов, обеспечить управляемость информационной системы, ее способность развиваться и противостоять новым угрозам при сохранении производительности и удобства использования. Опасность обхода сервисов безопасности существует по двум причинам:

- при реализации системы защиты в виде совокупности сервисов может существовать способ миновать отдельные защитные средства, нарушая тем самым целостность планируемой цепочки сервисов безопасности (пример — наличие выходов, идущих в обход межсетевых экранов);
- при построении информационной системы в многоуровневой архитектуре типа клиент/сервер может существовать способ обхода одного или нескольких уровней, на которых сосредоточены средства защиты.

Важной частью *архитектурного принципа* является минимизация объема защитных средств, выносимых на клиентские системы, ввиду того что: для доступа в корпоративную сеть рабочие места имеют ограниченную функциональность; а самое главное то, что конфигурацию клиентских рабочих мест трудно или невозможно контролировать.

Важность принципа *простоты архитектуры* доказана всем ходом развития информационных технологий, кризисами программирования, неудачами при создании больших систем. Следует стремиться к минимизации числа связей между компонентами информационной системы, поскольку именно оно определяет сложность. Однако, с принципом *простоты архитектуры* конфликтует необходимость внесения в систему определенной избыточности, обеспечивающей устойчивость по отношению к сбоям и отказам.

Сервисы безопасности

Рассмотрим более подробно основные сервисы безопасности.

Идентификация и аутентификация. Средства идентификации и аутентификации должны удовлетворять двум условиям:

- быть устойчивыми к пассивному и активному прослушиванию сети (сетевым угрозам);
- поддерживать концепцию единого входа в систему.

Первое требование можно выполнить, используя различные криптографические методы, в том числе и шифрование трафика. Однако более надежными методами являются подходы, основанные на протоколе Kerberos (поддержка этого протокола реализована во многих ОС) в сочетании со службой каталогов с сертификатами в стандарте X.509.

Единый вход в сеть — это, в первую очередь, требование удобства для пользователей. Если в корпоративной сети много информационных сервисов, допускающих независимое

обращение, то многократная идентификация/аутентификация становится слишком обременительной.

Существует несколько способов реализации службы идентификации/аутентификации. К первой относится, например, традиционная для приложений в различных ОС децентрализованная схема, предусматривающая аутентификацию каждого приложения. Отсутствие целостности и централизации в этой схеме затрудняет ее администрирование. Не обеспечивается гибкость в применении различных механизмов (способов) аутентификации, так как в этом случае требуется перекомпиляция приложения. Второй способ основан на библиотеке встроенных интерактивных модулей PAM (Pluggable Authentication Modules), являющейся частью ОС Red Hat Linux, представляет собой целостную централизованную систему, обеспечивающую гибкое использование различных механизмов аутентификации. Узким местом этого способа аутентификации и библиотеки PAM является обязательное требование интерактивности, что не всегда реализуемо на гетерогенной сетевой среде, и относительно сложный прикладной интерфейс.

Перспективы развития служб идентификации и аутентификации, особенно с учетом их применения для распределенных (информационных и вычислительных) систем, связаны с устранением отмеченных недостатков, а также разработкой новых способов, которые позволяли бы:

- учесть потребности перспективных направлений использования (корпоративный интранет, порталы, распределенные вычислительные метакомпьютерные системы типа GRID и т. п.);
- изыскать (разработать и апробировать) эффективные механизмы аутентификации для отмеченных выше идентификаторов второго и, особенно, третьего классов;
- надежно поддерживать не только традиционную конфиденциальность и целостность данных, но и высокую доступность информации на гетерогенной сетевой среде;
- расширить функциональные возможности системы аутентификации с целью ее более эффективной интеграции с другими сервисами безопасности (разграничение доступа, криптография, протоколирование и аудит и др.);
- использовать механизмы, которые легко реализовать средствами ОС.

Эти задачи с решаются при использовании единого ввода в систему на основе службы каталогов. К сожалению, пока нельзя сказать, что единый вход в сеть стал нормой, доминирующие решения пока не сформировались. Дополнительные удобства создает применение биометрических методов аутентификации, основанных на анализе отпечатков (точнее, результатов сканирования) пальцев. В отличие от специальных карт, которые нужно хранить, пальцы «всегда под рукой» (правда, под рукой должен быть и сканер). Подчеркнем, что и здесь защита от нарушения целостности и перехвата с последующим воспроизведением осуществляется методами криптографии. Стандарт X.509 описывает процедуру аутентификации с использованием службы каталогов. Впрочем, наиболее ценной в стандарте оказалась не сама процедура, а ее служебный элемент — структура сертификатов, хранящих имя пользователя, криптографические ключи и сопутствующую информацию. Подобные сертификаты — важнейший элемент современных схем аутентификации и контроля целостности.

Разграничение доступа. Разграничение доступа, вероятно, является самой исследованной областью информационной безопасности. «Дискреционное» и «мандатное» управление вошли во все теоретические курсы и критерии оценки. Доминируют они и на практике. К сожалению, в настоящее время следует признать устаревшим (или, по крайней мере, не полностью соответствующим действительности) положение о том, что разграничение доступа направлено на защиту от злоумышленных пользователей. Современные информационные системы характеризуются чрезвычайной сложностью и их внутренние ошибки представляют не меньшую опасность. Динамичность современной программной среды в сочетании со сложностью отдельных компонентов существенно сужает область

применимости самой употребительной — дискреционной модели управления доступом (называемой также моделью с произвольным управлением). При определении допустимости доступа важно не только (и не столько) то, кто обратился к объекту, но и то, какова семантика действия. Без привлечения семантики нельзя выявить троянские программы, противостоять которым произвольное управление доступом, как известно, не в состоянии. В последнее время появляются новые модели управления доступом, например, модель «песочницы» в Java-технологии. К сожалению, и она не учитывает семантику программ, что, на наш взгляд, является основной причиной выявляемых слабостей в системе безопасности. Активно развиваемое ролевое управление доступом решает не столько проблемы безопасности, сколько улучшает управляемость систем (что, конечно, очень важно). Суть его в том, что между пользователями и их привилегиями помещаются промежуточные сущности — роли. Для каждого пользователя одновременно могут быть активными несколько ролей, каждая из которых дает ему определенные права.

Мы уже отмечали, что сложность информационной системы характеризуется, прежде всего, числом имеющихся в ней связей. Поскольку ролей много меньше, чем пользователей и привилегий, их (ролей) использование способствует понижению сложности и, следовательно, улучшению управляемости. Кроме того, на основании ролевой модели можно реализовать такие важные принципы, как разделение обязанностей (невозможность в одиночку скомпрометировать критически важный процесс). Между ролями могут быть определены статические или динамические отношения несовместимости (невозможности одному субъекту по очереди или одновременно активизировать обе роли), что и обеспечивает требуемую защиту.

Протоколирование/аудит. Протоколирование/аудит традиционно являлись последним рубежом обороны, обеспечивающим анализ последствий нарушения информационной безопасности и выявление злоумышленников. Такой аудит можно назвать пассивным. Довольно очевидным обобщением пассивного аудита для сетевой среды является совместный анализ регистрационных журналов отдельных компонентов на предмет выявления противоречий, что важно в случаях, когда злоумышленнику удалось отключить протоколирование или модифицировать журналы.

В современный арсенал защитных средств несколько лет назад вошел активный аудит, направленный на выявление подозрительных действий в реальном масштабе времени. Активный аудит включает два вида действий:

- выявление нетипичного поведения (пользователей, программ или аппаратуры);
- выявление начала злоумышленной активности.

Нетипичное поведение выявляется статистическими методами, путем сопоставления с предварительно полученными образцами. Начало злоумышленной активности обнаруживается по совпадению с сигнатурами известных атак. За обнаружением следует заранее запрограммированная реакция (как минимум — информирование системного администратора, как максимум — контратака на систему предполагаемого злоумышленника).

Важным элементом современной трактовки протоколирования/аудита является протокол автоматизированного обмена информацией о нарушениях безопасности между корпоративными системами, подключенными к одной внешней сети. Работа над этим протоколом ведется под эгидой IETF. В наше время системы не могут считаться изолированными, они не должны жить по закону «каждый за себя»; угрозам следует противостоять сообща.

Протоколирование и аудит в системах ИБ обеспечивают возможности для реконструкции прошедших событий и их анализа с целью выявления нарушений, выработки мер к недопущению (исключению) деструктивных воздействий на объект защиты. Степень (объем) применения этого вида сервиса определяется политикой безопасности продукта или системы ИТ. С развитием и усложнением объектов защиты функции этого традиционного вида

сервиса значительно расширились. В условиях отсутствия гарантированно защищенных ОС, невозможности практического пресечения организации скрытых каналов передачи данных, особенно для распределенных систем в Интернет, а также целого ряда других «объективных уязвимостей» в традиционном комплексе средств защиты, подсистемы активного аудита способны существенно повысить уровень безопасности продуктов и систем ИТ. Оперативно анализируя разноплановые результаты протоколов о состоянии подлежащего защите объекта, такая подсистема призвана оперативно обнаружить попытку (потенциальную угрозу) деструктивного воздействия и выработать меры по его предотвращению.

Исследования и разработка подходов к совершенствованию компонент мониторинга состояния подконтрольной системы, механизмов и моделей анализа информации на каждом из ее уровней является очень важным направлением.

Описание и программная реализация такой существенно распределенной подсистемы на гетерогенной среде, выполняющей сбор большого объема разноплановых данных представляет собой самостоятельную задачу, соизмеримую по сложности с описанием и программным обеспечением системы в целом.

К числу основных задач на этом пути следует отнести:

- описание архитектуры подсистемы, эффективно сочетающей традиционные механизмы протоколирования с нетрадиционными способами организации, оперативного поиска и манипулирования полученными данными;
- исследования и выбор технических средств, алгоритмических решений, способных эффективно реализовать обработку больших объемов данных мониторинга.

К разряду перспективных, с точки зрения повышения эффективности подсистем активного аудита, относится задача, связанная с реализацией механизмов и моделей анализа данных о сетевом трафике, получаемых методами активного мониторинга. На этом направлении необходимо:

- исследовать закономерности в поведении сетевого трафика при «нормальном» режиме функционирования системы, сформулировать математические методы и модели, адекватно описывающие систему в таком состоянии;
- выбрать эффективные способы выявления «отклонений» системы от «нормы», их причины и своевременного реагирования на эти отклонения.

Экранирование. Экранирование как сервис безопасности выполняет следующие функции:

- разграничение межсетевого доступа путем фильтрации передаваемых данных;
- преобразование передаваемых данных.

Современные межсетевые экраны фильтруют данные на основе заранее заданной базы правил, что позволяет, по сравнению с традиционными операционными системами, реализовывать гораздо более гибкую политику безопасности. При комплексной фильтрации, охватывающей сетевой, транспортный и прикладной уровни, в правилах могут фигурировать сетевые адреса, количество переданных данных, операции прикладного уровня, параметры окружения (например, время) и т.п. Преобразование передаваемых данных может затрагивать как служебные поля пакетов, так и прикладные данные.

В первом случае обычно имеется в виду трансляция адресов, помогающая скрыть топологию защищаемой системы. Это — уникальное свойство сервиса экранирования, позволяющее скрывать существование некоторых объектов доступа. Преобразование данных может состоять, например, в их шифровании.

В процессе фильтрации (точнее, параллельно с ней) может выполняться дополнительный контроль (например, антивирусный). Возможны и дополнительные преобразования, наиболее актуальным из которых является исправление заголовков или иной служебной информации.

Туннелирование. На наш взгляд, туннелирование, как и экранирование, следует рассматривать как самостоятельный сервис безопасности. Его суть состоит в том, чтобы

«упаковать» передаваемую порцию данных, вместе со служебными полями, в новый «конверт». Данный сервис может применяться для нескольких целей:

- осуществление перехода между сетями с разными протоколами (например, IPv4 и IPv6);
- обеспечение конфиденциальности и целостности всей передаваемой порции, включая служебные поля.

Туннелирование может применяться как на сетевом, так и прикладном уровнях. Например, стандартизовано туннелирование для IP и двойное конвертование для почты X.400.

Комбинация туннелирования и шифрования (с необходимой криптографической инфраструктурой) на выделенных шлюзах позволяет реализовать такое важное в современных условиях защитное средство, как виртуальные частные сети. Такие сети, наложенные обычно поверх Интернет, существенно дешевле и гораздо безопаснее, чем действительно собственные сети организации, построенные на выделенных каналах. Коммуникации на всем их протяжении физически защитить невозможно, поэтому лучше изначально исходить из предположения об уязвимости и соответственно обеспечивать защиту. Современные протоколы, направленные на поддержку классов обслуживания, помогут гарантировать для виртуальных частных сетей заданную пропускную способность, величину задержек и т.п., ликвидируя тем самым единственное на сегодняшний день реальное преимущество сетей собственных.

Шифрование. Шифрование — важнейшее средство обеспечения конфиденциальности и, одновременно, самое конфликтное место информационной безопасности (практически во всех странах, не только в России).

Контроль целостности. Контроль целостности относится к числу "благополучных" сервисов безопасности, несмотря на его криптографическую природу. Здесь и проблема производительности стоит не так остро, как в случае шифрования, и отечественные стандарты лучше согласуются с международными. В современных системах контроль целостности должен распространяться не только на отдельные порции данных, аппаратные или программные компоненты. Он обязан охватывать распределенные конфигурации, защищать от несанкционированной модификации потоки данных. В настоящее время существует достаточно решений для контроля целостности и с системной, и с сетевой направленностью (обычно контроль выполняется прозрачным для приложений образом как часть общей протокольной активности).

Контроль защищенности. Контроль защищенности по сути представляет собой попытку «взлома» информационной системы, осуществляемого силами самой организации или уполномоченными лицами. Идея данного сервиса в том, чтобы обнаружить слабости в защите раньше злоумышленников. В первую очередь, имеются в виду не архитектурные (их ликвидировать сложно), а «оперативные» бреши, появившиеся в результате ошибок администрирования или из-за невнимания к обновлению версий программного обеспечения.

Средства контроля защищенности позволяют накапливать и многократно использовать знания об известных атаках. Очевидна их схожесть с антивирусными средствами; формально последние можно считать их подмножеством. Очевиден и реактивный, запаздывающий характер подобного контроля (он не защищает от новых атак). Впрочем, следует помнить, что оборона должна быть эшелонированной, так что в качестве одного из рубежей контроль защищенности вполне адекватен. Отметим также, что подавляющее большинство атак носит рутинный характер; они возможны только потому, что известные слабости годами остаются неустраненными.

Существуют как коммерческие, так и свободно распространяемые продукты для контроля защищенности. Впрочем, в данном случае важно не просто один раз получить и установить их, но и постоянно обновлять базу данных слабостей. Это может оказаться не проще, чем следить за информацией о новых атаках и рекомендуемых способах противодействия.

Обнаружение отказов и оперативное восстановление. Обнаружение отказов и оперативное восстановление относится к числу сервисов, обеспечивающих высокую доступность (готовность). Его работа опирается на элементы архитектурной безопасности, а именно на существование избыточности в аппаратно-программной конфигурации.

В настоящее время спектр программных и аппаратных средств данного класса можно считать сформировавшимся. На программном уровне соответствующие функции берет на себя программное обеспечение промежуточного слоя. Среди аппаратно-программных продуктов стандартом стали кластерные конфигурации. Восстановление производится действительно оперативно (десятки секунд, в крайнем случае минуты), прозрачным для приложений образом. Важно отметить, что обнаружение отказов и оперативное восстановление может играть по отношению к другим средствам безопасности инфраструктурную роль, обеспечивая высокую готовность последних. Это особенно важно для межсетевых экранов, средств поддержки виртуальных частных сетей, серверов аутентификации, нормальное функционирование которых критически важно для корпоративной информационной системы в целом. Такие комбинированные продукты получают все более широкое распространение.

Управление. Управление можно отнести к числу инфраструктурных сервисов, обеспечивающих нормальную работу функционально полезных компонентов и средств безопасности. Сложность современных систем такова, что без правильно организованного управления они постепенно (а иногда и довольно быстро) деградируют как в плане эффективности, так и в плане защищенности.

Особенно важной функцией управления является контроль согласованности конфигураций различных компонентов (имеется в виду семантическая согласованность, относящаяся, например, к наборам правил нескольких межсетевых экранов). Процесс администрирования идет постоянно; требуется, однако, чтобы при этом не нарушалась политика безопасности.

Современное управление, на наш взгляд, вступило в переломный этап. Начинают появляться продукты, обладающие достаточной интеллектуальностью, открытостью, расширяемостью, масштабируемостью, продукты, приемлемые по цене и по потребляемым ресурсам. Вероятно, должно пройти еще некоторое время, чтобы они стали достаточно зрелыми, стабилизировались.

Политики безопасности

Для выполнения требований информационной безопасности необходим поиск новых способов к формализации политик безопасности (ПБ). К их числу можно отнести следующие:

- Разработку новых или эффективное использование уже существующих языков моделирования, позволяющих на концептуальном уровне построения модели ПБ отобразить семантику проблемной области. Такие модельно-языковые средства способны обеспечить более адекватное (полное и математически строгое) описание моделей систем, реализующих заданную ПБ и, как следствие, доказательную базу ее гарантированной защищенности.
- Создание моделей ПБ, учитывающих специфику распределенных систем на гетерогенной среде Интернет, использующих в качестве базовых графовые и автоматные, статистические, детерминированные и другие, как традиционные так и нетрадиционные способы их формализации. Учет факторов, характеризующих описанные выше особенности больших распределенных систем, будет также способствовать совершенствованию доказательной базы их гарантированной защищенности.
- Разработка подходов к построению моделей ПБ на основе совершенствования традиционных - произвольного (дискреционная модель), принудительного

(мандатный контроль), ролевого доступа и их комбинации для различных структурных элементов (компонентов), сервисов и приложений больших распределенных систем. Рациональное использование различных моделей в составе больших систем способно повысить уровень их защищенности, сократить время и обеспечить экономию вычислительных ресурсов на реализацию мер, предусмотренных ПБ.

Заключение

Анализируя основные проблемы информационной безопасности в крупной научно-образовательной сети, какой является СПД СО РАН, можно выделить две основные задачи, вторая из которых, вообще говоря, вытекает из первой. Первая задача — задача четкого управления информационными ресурсами, включающая в том числе задачи идентификации, аутентификации и разграничения доступа к ресурсами. Вторая — контроль за использованием информационными ресурсами.

Создание и поддержка распределенных информационных систем и электронных библиотек, интегрирующих разнородные информационные ресурсы и функционирующих в различных программно-аппаратных средах, требует специальных подходов к управлению этими системами. Если управление собственно самими ресурсами или данными может осуществляться в локальном режиме даже для распределенных информационных систем, то задача управления доступом к распределенным ресурсам не может быть решена в рамках локального администрирования. Выбор технологии, основанной на службе каталогов (LDAP) для построения Системы управления распределенными информационными ресурсами применительно к СПД СО РАН изложен в статье [4]. Вторая задача может быть решена путем создания технологий построения эффективных распределенных программных систем для обеспечения информационной безопасности крупных корпоративных сетей [5]. Такие системы должны обеспечивать обнаружение внутренних и внешних угроз и вторжений, фильтрацию внешнего трафика, контроль за использованием корпоративных сетевых ресурсов и предотвращение утечек конфиденциальной информации. Входными данными при этом является информация о структуре и характеристиках трафика (прецедентная информация), позволяющая построить набор правил, классифицирующих нормальные или аномальные компоненты трафика. В этом направлении следует ожидать существенное повышение безопасности сетей за счет оперативного реагирования на набор известных угроз и на ранее не встречавшиеся аномальные ситуации, а также за счет идентификации реально функционирующих сетевых приложений или процессов и управления ими для обеспечения доступности информационных сервисов необходимых сетевому сообществу.

Мероприятия по обеспечению информационной безопасности, как известно, не приносят доходов, с их помощью можно лишь уменьшить ущерб от возможных инцидентов. Поэтому очень важно, чтобы затраты на создание и поддержание информационной безопасности на должном уровне были соразмерны ценности активов организации, связанных с ее информационной системой (ИС). Соразмерность может быть обеспечена категорированием информации и информационной системы, а также выбором регуляторов безопасности на основе результатов категорирования.

Литература

1. Сеть передачи данных СО РАН // Информационные материалы научно-координационного совета целевой программы «Информационно-телекоммуникационные ресурсы СО РАН», Новосибирск, 2005.
2. Шокин Ю.И., Федотов А.М. Организация и поддержка информационно-вычислительных ресурсов СО РАН // Сб. научных трудов. Инновационные недра Кузбасса. IT-технологии. – Кемерово, ИНТ, 2007. С. 30-34.

3. Scarfone, K. Guide to Intrusion Detection and Prevention Systems (IDPS). Recommendations of the National Institute of Standards and Technology / Karen Scarfone, Peter Mell; Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology Special Publication 800-94. – Gaithersburg, 2007. – 127 p.
4. Жижимов О.Л., Федотов А.М. Модели управления доступом к распределенным информационным ресурсам // Труды IX Всероссийской научной конференции RCDL'2007, 15-18 октября 2007 г. Переславль-Залесский. С.296-299.
5. Белов С. Д., Жижимов О.Л., Попов Д.С., Чубаров Л. Б, Федотов А.М. Подходы к анализу потоков данных и идентификации приложений в крупных научно образовательных сетях // Труды Второй международной конференции «Системный анализ и информационные технологии» САИТ-2007 (Обнинск, Россия, 10-14 сентября 2007, С. 174-178.