Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 8 (75)/1999

Активный аудит

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Активный аудит

Алексей Галатенко
мех-мат МГУ

СОДЕРЖАНИЕ

1. Введение

Все связи на этой земле распались.
И имена потеряли смысл. Остался лишь мир, полный угрозы, мир, лишенный имени и потому таивший в себе безымянные опасности, которые подстерегали тебя на каждом шагу. Опасности эти не обрушивались на человека сразу, не хватали его за горло, не валили с ног — нет, они были куда ужасней, ибо они подкрадывались беззвучно, незаметно.

Э.М. Ремарк. «Тени в раю»

Статьи по информационной безопасности принято начинать с нагнетания страстей. Мы не станем отступать от этой недоброй традиции.

В марте 1999 года был опубликован очередной, четвертый по счету, годовой отчет «Компьютерная преступность и безопасность-1999: проблемы и тенденции» («Issues and Trends: 1999 CSI/FBI Computer Crime and Security Survey»), подготовленный Институтом компьютерной безопасности (Computer Security Institute, CSI) во взаимодействии с отделением Федерального бюро расследований по Сан-Франциско (см. [1]).

В отчете констатируется резкий рост числа обращений в правоохранительные органы по поводу компьютерных преступлений (32% из числа опрошенных). 30% респондентов сообщили о том, что их информационные системы были взломаны внешними злоумышленниками. Атакам через Интернет подвергались 57% опрошенных. 55% отметили нарушения со стороны собственных сотрудников. Примечательно, что 33% респондентов на вопрос «были ли взломаны ваши Web-серверы и системы электронной коммерции за последние 12 месяцев?» ответили «не знаю».

Столь же тревожные результаты содержатся в обзоре InformationWeek, опубликованном 12 июля 1999 года (см. [2]). Лишь 22% заявили об отсутствии нарушений информационной безопасности. Наряду с распространением вирусов отмечен резкий рост числа внешних атак.

К сожалению, не составляет труда продолжить эту мрачную статистику, однако, на наш взгляд, для первичной оценки общей картины приведенных цифр вполне достаточно.

Увеличение числа атак — это только одно из зол (вероятно, меньшее). Хуже то, что постоянно обнаруживаются новые слабости в программном обеспечении и, как следствие, появляются новые способы проведения атак. Так, в информационном письме Национального центра защиты инфраструктуры США (National Infrastructure Protection Center, NIPC) от 21 июля 1999 года сообщается, что за период с 3 по 16 июля 1999 года выявлено девять проблем с ПО, риск использования которых оценивается как средний или высокий (общее число обнаруженных слабостей равно 17, см. [3]). Среди «пострадавших» операционных платформ — почти все разновидности ОС Unix, Windows, MacOS, так что никто не может чувствовать себя спокойно, поскольку новые слабости тут же начинают интенсивно эксплуатироваться.

В таких условиях системы информационной безопасности должны уметь противостоять многочисленным, разнообразным атакам, ведущимся изнутри и извне, атакам автоматизированным и скоординированным. Иногда нападение длится доли секунды; порой прощупывание слабостей ведется медленно и растягивается на часы, так что подозрительная активность практически незаметна. Целью злоумышленников может быть нарушение доступности, целостности или конфиденциальности.

Темой настоящей статьи является относительно новый сервис безопасности — активный аудит (систематическое рассмотрение сервисов безопасности можно найти, например, в [4]). Активный аудит направлен на выявление подозрительной (злоумышленной и/или аномальной) активности с целью оперативного принятия ответных мер. С этим сервисом связываются надежды на существенное повышение защищенности корпоративных информационных систем (может быть, потому, что недостаточность более традиционных механизмов, к сожалению, доказана практикой).

Позволим себе привести еще несколько цифр. По данным исследовательского органа конгресса США, General Accounting Office (GAO), в 1996 финансовом году на федеральные компьютерные системы было предпринято около 250 тысяч атак, 65% которых (160 тысяч) оказались успешными (см. [5]). Это плохо, как плохо и то, что число атак каждый год удваивается. Но гораздо хуже, что было выявлено лишь 4% успешных атак, из которых только о 27% были составлены доклады. Очевидно, нужно снижать процент успешных атак (если нет возможности повлиять на их общее число) и резко увеличивать процент «раскрываемости». Активный аудит может помочь в достижении обеих целей.

Данная статья основана как на изучении многочисленных зарубежных и (менее многочисленных) отечественных источников, так и на личном опыте автора, полученном при создании и пробной эксплуатации системы активного аудита в НИИ системных исследований Российской академии наук.

Для русскоязычных публикаций по информационным технологиям традиционно трудной является терминологическая проблема. Мы предлагаем «активный аудит» в качестве эквивалента английского «intrusion detection» (выявление вторжений). На наш взгляд, термин «активный аудит» верно отражает суть дела и даже содержит некоторый запас общности по сравнению «intrusion detection», поскольку речь идет не только о выявлении, но и об отражении вторжений.

2. Активный аудит и его место среди других сервисов безопасности

Высшая цель прилежного коммерсанта заключается в том, чтобы не только содрать с клиента шкуру, но и заставить его благодарить за это.
Э.М. Ремарк. «Тени в раю»

Формула «защищать, обнаруживать, реагировать» (по-английски это звучит лучше: «protect, detect, react») является классической. Только эшелонированная, активная оборона, содержащая разнообразные элементы, дает шанс на успешное отражение угроз.

Назначение активного аудита — обнаруживать и реагировать. Как указывалось во введении, обнаружению подлежит подозрительная активность компонентов информационной системы (ИС) — от пользователей (внутренних и внешних) до программных систем и аппаратных устройств.

Подозрительную активность можно подразделить на злоумышленную и аномальную (нетипичную). Злоумышленная активность — это либо атаки, преследующие цель несанкционированного получения привилегий, либо действия, выполняемые в рамках имеющихся привилегий (возможно, полученных незаконно), но нарушающие политику безопасности. Последнее мы будем называть злоупотреблением полномочиями. Нетипичная активность может впрямую не нарушать политику безопасности, но, как правило, она является следствием либо некорректной (или сознательно измененной) работы аппаратуры или программ, либо действий злоумышленников, маскирующихся под легальных пользователей.

Активный аудит дополняет такие традиционные защитные механизмы, как идентификация/аутентификация и разграничение доступа. Подобное дополнение необходимо по двум причинам. Во-первых, существующие средства разграничения доступа не способны реализовать все требования политики безопасности, если по-

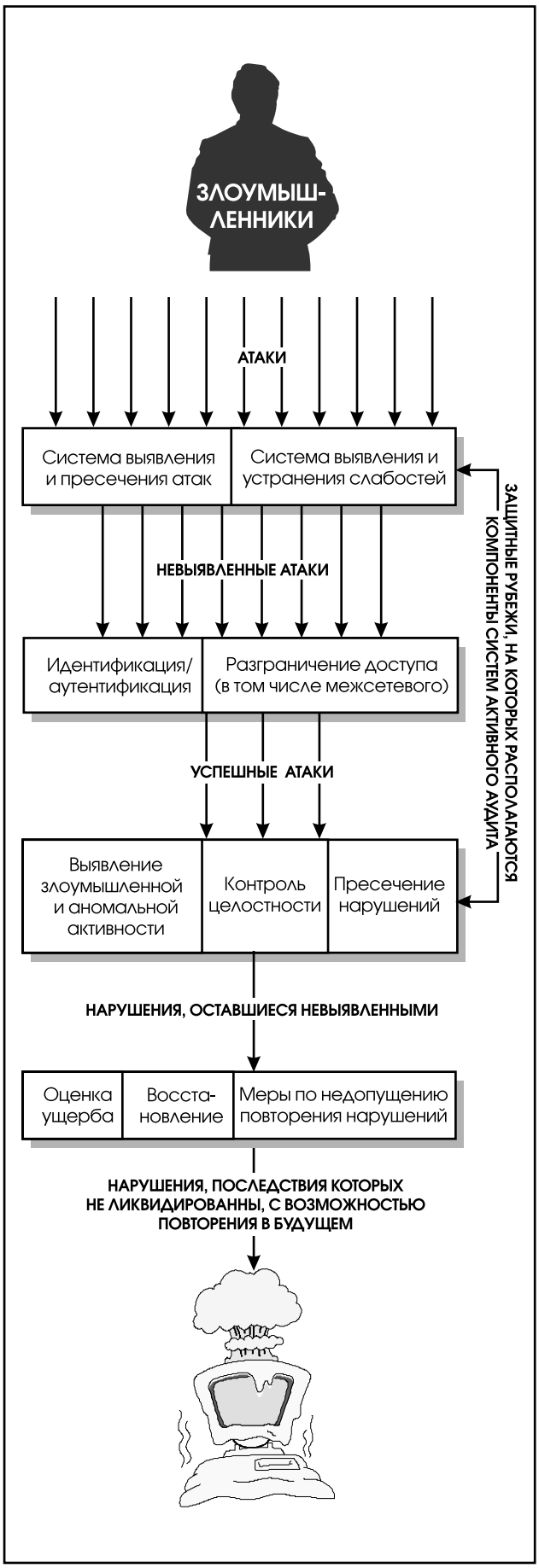

Рис. 1. Защитные рубежи, контролируемые системами активного аудита.

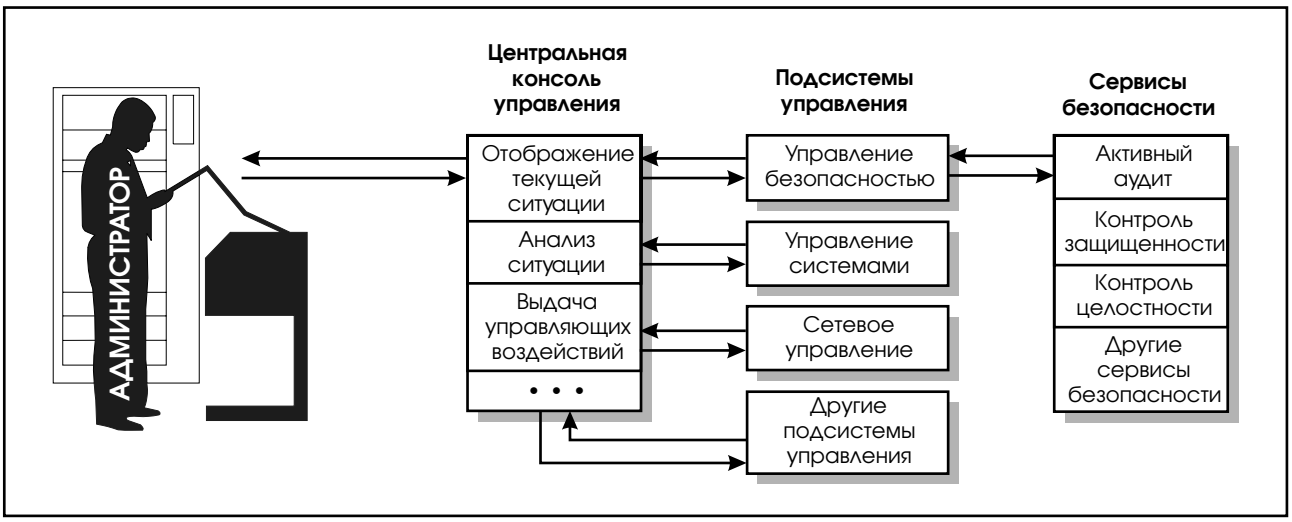

Рис. 2. Интеграция сервисов безопасности и системы управления.

следние имеют более сложный вид, чем разрешение/запрет атомарных операций с ресурсами. Развитая политика безопасности может накладывать ограничения на суммарный объем прочитанной информации, запрещать доступ к ресурсу B, если ранее имел место доступ к ресурсу A, и т.п. Во-вторых, в самих защитных средствах есть ошибки и слабости, поэтому, помимо строительства заборов, приходится заботиться об отлавливании тех, кто смог через эти заборы перелезть.

Развитые системы активного аудита несут двойную нагрузку, образуя как первый, так и последний защитные рубежи (см. рис. 1). Первый рубеж предназначен для обнаружения атак и их оперативного пресечения. На последнем рубеже выявляются симптомы происходящих в данный момент или ранее случившихся нарушений политики безопасности, принимаются меры по пресечению нарушений и минимизации ущерба.

И на первом, и на последнем рубеже, помимо активного аудита, присутствуют другие сервисы безопасности. К первому рубежу можно отнести сканеры безопасности, помогающие выявлять и устранять слабые места в защите. На последнем рубеже для обнаружения симптомов нарушений могут использоваться средства контроля целостности. Иногда их включают в репертуар систем активного аудита; мы, однако, не будем этого делать, считая контроль целостности отдельным сервисом.

Между сервисами безопасности существуют и другие связи. Так, активный аудит может опираться на традиционные механизмы протоколирования. В свою очередь, после выявления нарушения зачастую требуется просмотр ранее накопленной регистрационной информации, оценить ущерб, понять, почему нарушение стало возможным, спланировать меры, исключающие повторение инцидента. Параллельно производится надежное восстановление первоначальной (то есть не измененной нарушителем) конфигурации.

Отдельным вопросом является взаимодействие систем активного аудита и управления. Активный аудит выполняет типичные управляющие функции — анализ данных об активности в информационной системе, отображение текущей ситуации, автоматическое реагирование на подозрительную активность. Сходным образом функционирует, например, подсистема сетевого управления. На наш взгляд, целесообразно интегрировать активный аудит и «общее» управление, в максимально возможной степени используя общие программно-технические и организационные решения. В эту интегрированную систему может быть включен и контроль целостности, а также агенты другой направленности, отслеживающие специфические аспекты поведения ИС (см. рис. 2).

С логической точки зрения можно считать, что существует центральная консоль управления, куда стекаются данные от систем активного аудита, контроля целостности, анализа защищенности, контроля систем и сетей по другим аспектам. На этой консоли в том или ином виде отображается текущая ситуация, с нее, автоматически или вручную, выдаются управляющие команды. В силу технических или организационных причин эта консоль физически может быть реализована в виде нескольких рабочих мест (с выделением, например, места администратора безопасности), но суть дела от этого не меняется.

К сближению управления и сервисов безопасности движутся обе стороны. Так, в продукте компании Computer Associates CA-Unicenter (см. [6]) имеется мощная подсистема

управления безопасностью, а новейшая разработка — нейроагенты — использует методы, типичные при выявлении подозрительной активности.

С другой стороны, один из самых известных специалистов в области информационной безопасности Маркус Ранум (Markus Ranum) призывает «безопасников» отказаться от трактовки их дисциплины как чего-то изолированного от сетевого управления. «Обнаружение ошибок, вторжений или отказов — все это аспекты единой проблемы управления сетями» — указывает он (см. [7]).

Сам Ранум следует собственным рекомендациям, рассматривая продукт для активного аудита NFR (Network Flight Recorder) как компонент системы сетевого управления с соответствующей реализацией.

В последующих разделах мы еще не раз будем затрагивать архитектурные вопросы, без решения которых невозможно создать результативную, гибкую, масштабируемую систему активного аудита.

3. Методы проведения активного аудита

В этот период она походила на генерала, который сводит воедино донесения о мелких боевых эпизодах и наносит их на большую карту. Ничто не ускользает от его внимания, он сравнивает, проясняет неясности, регистрирует факты, и вот перед его глазами встает вся картина сражения; вокруг него люди празднуют победу и с оптимизмом смотрят в будущее, но генерал уже знает, что сражение проиграно, и, невзирая на победные реляции профанов, он собирает свое войско, чтобы повести его на последний штурм!

Э.М. Ремарк. «Тени в раю»

3.1. Немного истории

Первые работы в области систем активного аудита относятся к началу 1980-х годов (см. [8]). До этого регистрационная информация обрабатывалась вручную (во всяком случае, без применения специального программного обеспечения) штатом аудиторов. Работа людей-аудиторов была тяжелой и неэффективной; очевидно, в наше время вдвойне наивно надеяться на то, что системный администратор (даже высококвалифицированный) без средств активного аудита сможет в режиме реального времени найти в регистрационных журналах подозрительные записи и принять адекватные меры противодействия. К тому же найти системного администратора корпоративного уровня сейчас много сложнее, чем двадцать лет назад — квалифицированного аудитора.

Вполне понятно, что на первом этапе не было речи об анализе сетевой активности (самих сетей было не так много). Обрабатывались системные журналы, иногда с небольшой задержкой, чаще — раз в сутки (тогда подобные задержки были вполне приемлемыми). Направление сетевой безопасности стало интенсивно развиваться примерно десять лет спустя в 1990-е годы и плоды этого развития мы наблюдаем сейчас, прежде всего, на примере межсетевых экранов.

При разработке систем активного аудита вставали как концептуальные, так и технические проблемы. По большому счету концептуальная проблема была одна: как выявлять подозрительную активность? Первоначально были предложены статистические методы, основанные на предположении о том, что злоумышленная активность всегда сопровождается какими-то аномалиями, изменением профиля поведения пользователей, программ или аппаратуры. Несколько позднее для нужд активного аудита стали применять экспертные системы, описывающие злоумышленную активность совокупностью правил.

Довольно быстро стало понятно, что два подхода — статистический и экспертный — хорошо дополняют друг друга и что с возникающими проблемами они могут справиться только вместе. Действительно, статистический подход хорош там, где существует понятие типичного поведения, а распределения измеряемых величин в нормальной ситуации остаются относительно стабильными. С другой стороны, экспертный подход плохо справляется с неизвестными атаками (равно как и с многочисленными вариациями известных атак). В последующих разделах мы увидим, как могут выглядеть интегрированные системы активного аудита.

Главной технической проблемой является проблема масштабируемости. Даже на одном хосте при числе пользователей порядка нескольких сотен объем регистрационной информации, генерируемой только операционной системой, измеряется гигабайтами или в лучшем случае сотнями мегабайт. Хранение и обработка подобных объемов — задача непростая. Если же система становится распределенной, то проблемы начинают нарастать гораздо быстрее, чем число компонентов.

Несмотря на все сложности, интенсивность работ в области активного аудита нарастает. Это касается и коммерческих, и исследовательских проектов.

В настоящее время число предлагаемых коммерческих систем составляет несколько де-

сятков. Согласно оценкам аналитиков, рынок средств активного аудита составлял в 1998 году в стоимостном выражении 100 миллионов долларов против 40 миллионов в 1997 году (см. [9]). Несомненно, в ближайшие годы высокие темпы расширения рынка сохранятся. В качестве оценок называют 150 миллионов долларов в 1999 году и более 600 миллионов в 2002 году (см. [10]).

По-видимому, исследовательские проекты в области активного аудита никогда не испытывали недостатка в средствах. В последние годы ситуация в этом смысле стала еще более благоприятной, поскольку выявление подозрительной активности было произведено в ранг «оборонительного информационного оружия». Согласно утверждению автора статьи [10], он участвовал в распределении 500 миллионов долларов, которые выделялись на 2000 год по линии Министерства энергетики США на исследования и разработки в области зловредного кода, аномальной активности и обнаружения вторжений. По российским меркам подобная активность явно попадает в разряд аномальных...

3.2. Архитектура систем активного аудита

У систем активного аудита целесообразно различать локальную и глобальную архитектуру. В рамках локальной архитектуры реализуются элементарные составляющие, которые затем могут быть объединены для обслуживания корпоративных систем.

Основные элементы локальной архитектуры и связи между ними показаны на рис. 3. Первичный сбор данных осуществляют агенты, называемые также сенсорами. Регистрационная информация может извлекаться из системных или прикладных журналов (технически несложно получать ее и напрямую от ядра ОС), либо добываться из сети с помощью соответствующих механизмов активного сетевого оборудования или путем перехвата пакетов посредством установленной в режим мониторинга сетевой карты.

На уровне агентов (сенсоров) может выполняться фильтрация данных с целью уменьшения их объема. Это требует от агентов некоторого интеллекта, но зато разгружает остальные компоненты системы.

Агенты передают информацию в центр распределения, который приводит ее к единому (стандартному для конкретной системы активного аудита) формату, возможно, осуществляет дальнейшую фильтрацию (редукцию), сохраняет в базе данных и направляет для анализа статистическому и экспертному компонентам. Один центр распределения может обслуживать несколько сенсоров.

Содержательный активный аудит начинается со статистического и экспертного компонентов (например, потому, что для однохостовых систем регистрационную информацию не надо каким-то особым образом извлекать и передавать). Мы детально рассмотрим их в двух следующих разделах.

Если в процессе статистического или экспертного анализа выявляется подозрительная

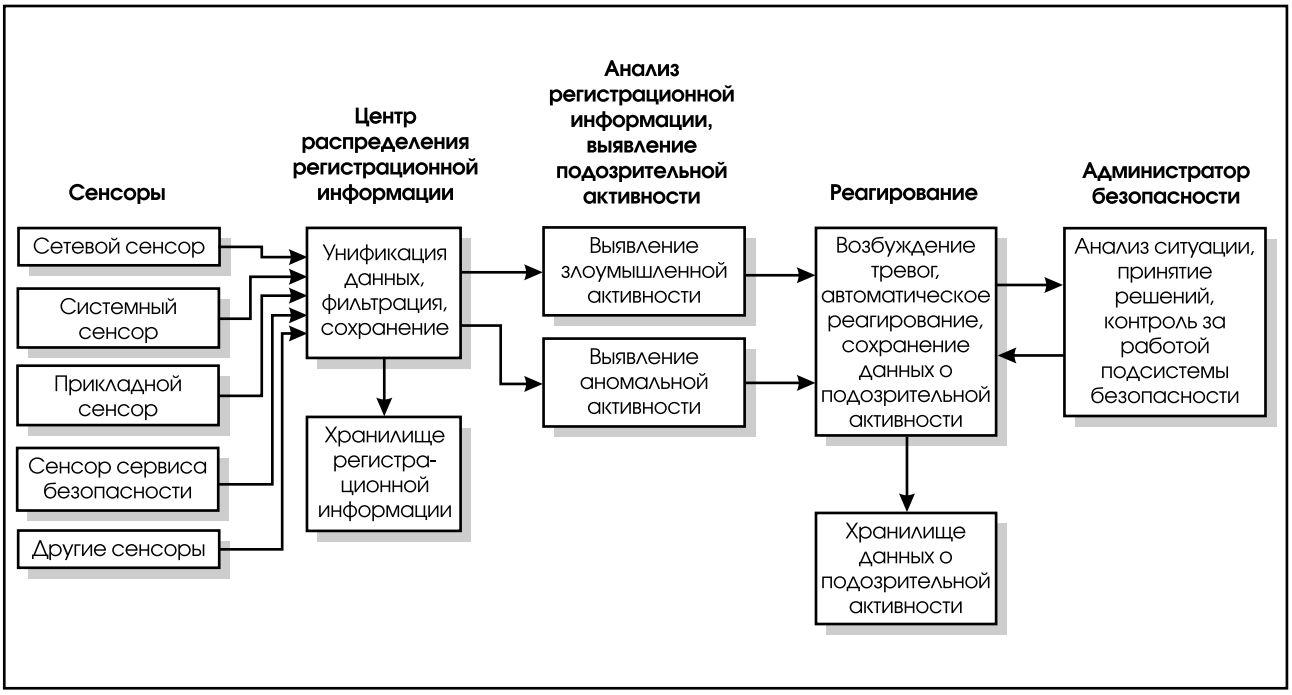

Рис. 3. Основные элементы локальной архитектуры систем активного аудита.

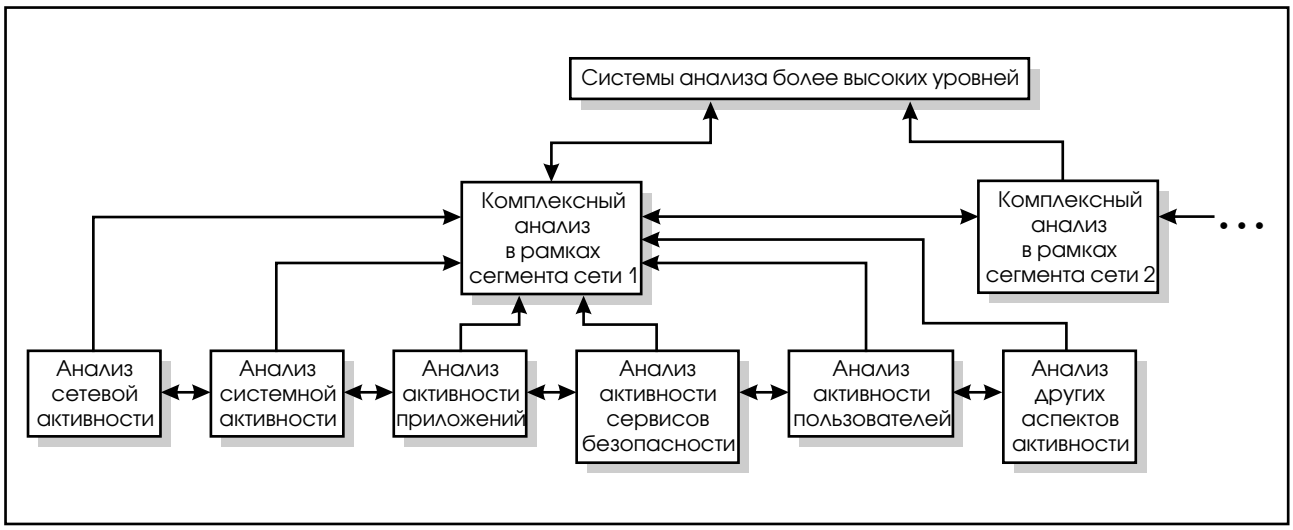

Рис. 4. Глобальная архитектура системы активного аудита.

активность, соответствующее сообщение направляется решателю, который определяет, является ли тревога оправданной, и выбирает способ реагирования.

Обычно, когда пишут о способах реагирования, перечисляют отправку сообщения на пейджер администратора, посылку электронного письма ему же и т.п., то есть имеют в виду «ручное» принятие мер после получения сигнала о подозрительной активности. К сожалению, многие современные атаки длятся секунды или даже доли секунды, поэтому включение в процесс реагирования человека вносит недопустимо большую задержку. Ответные меры должны быть в максимально возможной степени автоматизированы, иначе активность аудита во многом теряет смысл.

Автоматизация нужна еще и по той простой причине, что далеко не во всех организациях системные администраторы обладают достаточной квалификацией для адекватного реагирования на инциденты. Хорошая система активного аудита должна уметь внятно объяснить, почему она подняла тревогу, насколько серьезна ситуация и каковы рекомендуемые способы действия. Если выбор должен оставаться за человеком, то пусть он сводится к нескольким элементам меню, а не к решению концептуальных проблем.

Мы оставляем вне рамок нашего рассмотрения интерфейсы с СУБД (для хранения и обработки регистрационной информации), и с системами управления, поскольку это стандартные технические моменты, многократно описанные в литературе. Еще раз подчеркнем, что безопасность — это инфраструктурное свойство информационных систем. Сервисы безопасности должны быть интегрированы с другими инфраструктурными механизмами (управления, хранения и т.п.), иначе эксплуатация и развитие информационной системы окажутся крайне сложными и дорогостоящими.

Глобальная архитектура подразумевает организацию одноранговых и разноранговых связей между локальными системами активного аудита (см. рис. 4). На одном уровне иерархии располагаются компоненты, анализирующие подозрительную активность с разных точек зрения. Например, на хосте могут располагаться подсистемы анализа поведения пользователей и приложений. Их может дополнять подсистема анализа сетевой активности. Когда один компонент обнаруживает что-то подозрительное, то во многих случаях целесообразно сообщить об этом соседям либо для принятия мер, либо для усиления внимания к определенным аспектам поведения системы.

Разноранговые связи используются для обобщения результатов анализа и получения целостной картины происходящего. Иногда у локального компонента недостаточно оснований для возбуждения тревоги, но «по совокупности» подозрительные ситуации могут быть объединены и совместно проанализированы, после чего порог подозрительности окажется превышенным. Целостная картина, возможно, позволит выявить скоординированные атаки на разные участки информационной системы и оценить ущерб в масштабе организации.

Очевидно, формирование иерархии компонентов активного аудита необходимо и для решения проблем масштабируемости, но этот аспект является стандартным для систем управления и мы не будем на нем останавливаться.

К числу важнейших архитектурных относится вопрос о том, какую информацию и в каких масштабах собирать и анализировать. Первые системы активного аудита были однохостовыми. Затем появились многохостовые конфигурации. Прорыву в области коммерческих про-

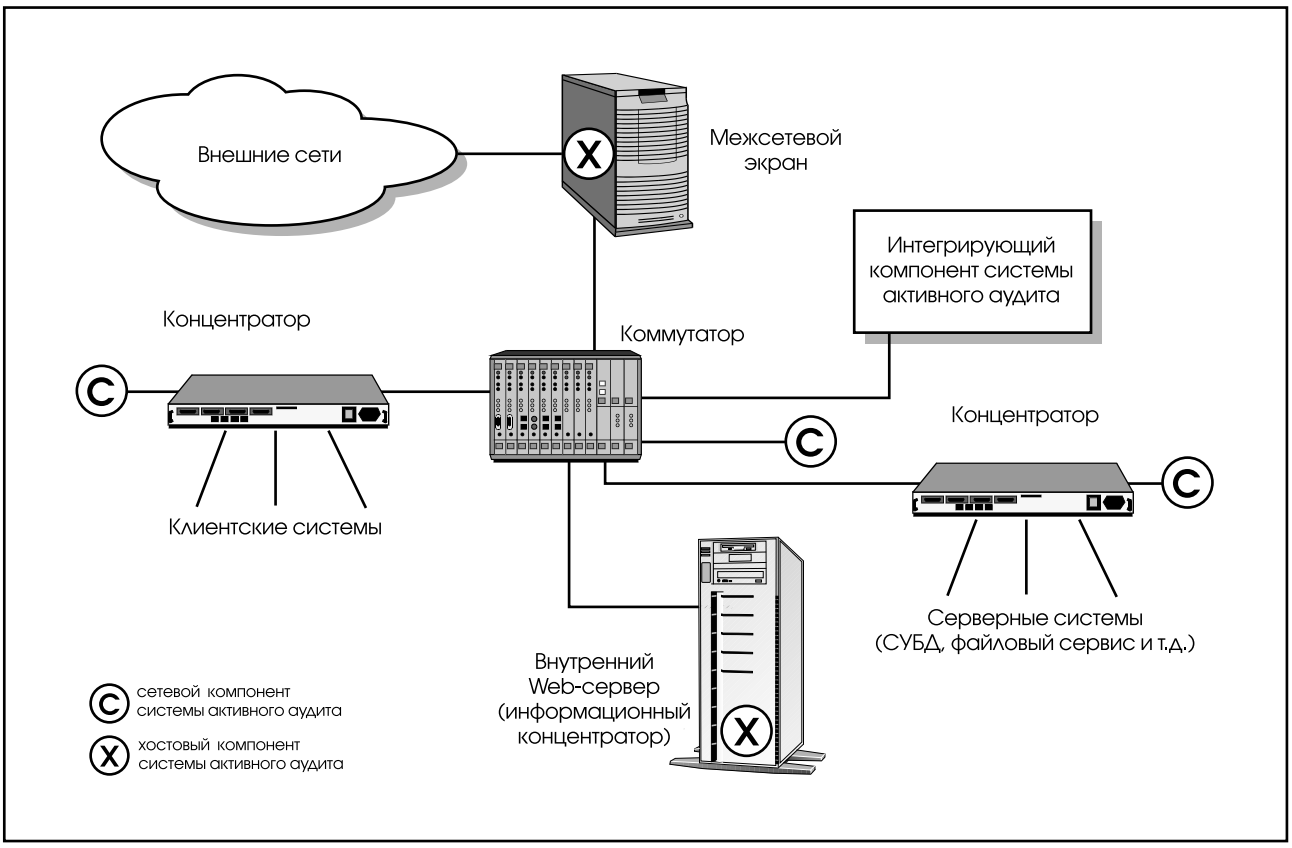

Рис. 5. Архитектура комплексной системы активного аудита.

дуктов мы обязаны сетевым системам, анализировавшим исключительно сетевые пакеты. Наконец, в настоящее время, как и следовало ожидать, можно наблюдать конвергенцию архитектур, в результате чего рождаются комплексные системы, отслеживающие и анализирующие как компьютерную, так и сетевую регистрационную информацию (см. рис. 5).

На наш взгляд, по многим причинам полезно представлять себе информационную систему как совокупность сервисов (а не сетей и узлов). Соответственно, нужно протоколировать и анализировать поведение сервисов независимо от места их локализации и степени распределенности. Сеть как таковая обеспечивает передачу данных (мы не берем сейчас в расчет дополнительные сетевые сервисы, это отдельный вопрос). Пытаться извлечь из сетевого трафика нечто большее (например, информацию о поведении приложений) нецелесообразно, да и невозможно (мы вернемся к этому вопросу в разделе, посвященном тестированию систем активного аудита). Даже в таком продвинутом продукте, как FireWall-1 компании CheckPoint, не удалось достичь полного успеха в деле фильтрации с восстановлением контекста — разграничение межсетевого доступа с точностью до команд прикладных протоколов осталось возможным только при применении «честных» proxy-сервисов. А ведь у межсетевых экранов цели анализа проще, чем у систем активного аудита!

Рискнем утверждать, что без понимания семантики защищаемых или анализируемых объектов обеспечение безопасности невозможно. Это понимание может быть выражено в процедурном (программы) или декларативном (описания) видах, но оно должно существовать. Декларативная семантика предпочтительнее, поскольку она позволяет без изменений применять программный продукт к различным объектам. Здесь опять-таки напрашивается аналогия с системами управления и административными информационными базами (MIB).

В статье [6] отмечалось, что современные информационные системы не готовы к эффективному управлению. В еще большей степени этот вывод применим к активному аудиту. Программные системы являются «неаудируемыми», нет ясных критериев, позволяющих отличить нормальное поведение от злоумышленного или аномального. В таких условиях наивно было бы ожидать, что установленные «поверх» средства выявления подозрительной активности сотворят чудо и отразят все атаки. Впрочем, вопрос «аудируемости» программных продуктов пока совершенно не исследован, и мы не будем на нем останавливаться.

Традиционным является вопрос, где размещать сенсоры систем активного аудита. Столь

же традиционный ответ гласит: «везде, где можно». Только анализ всех доступных источников информации позволит с достоверностью обнаруживать атаки и злоупотребления полномочиями и докапываться до их первопричин (см. [11]). Если вернуться к трактовке информационной системы в виде совокупности сервисов, то средства обнаружения атак должны располагаться перед защищаемыми ресурсами (имея в виду направление движения запросов к сервисам), а средства выявления злоупотреблений полномочиями — на самих сервисах. Обнаружение аномальной активности полезно во всех упомянутых точках. Только при таком размещении сенсоров будет выполнен важнейший принцип невозможности обхода защитных средств. Кроме того, будет минимизировано число сенсоров, что в условиях сегментации сетей и применения коммутационных технологий также оказывается проблемой.

К числу часто задаваемых относится и вопрос о том, как сочетать средства активного аудита (в первую очередь, сетевого) и межсетевые экраны. Разумеется, эти механизмы безопасности не исключают, а дополняют друг друга. Например, межсетевой экран бессилен против нелегальных модемных входов/выходов, а активный аудит позволяет обнаруживать их. Еще один вопрос — располагать ли средства выявления атак перед межсетевым экраном, чтобы защитить его. Любопытно, что за «круглым столом» [7] специалисты высказывали на этот счет прямо противоположные мнения. На наш взгляд, межсетевым экранам нужно доверять, они являются продуктом более зрелой технологии, чем коммерческие системы активного аудита. Конечно, целесообразно контролировать целостность конфигурации экрана, выявлять иные возможные аномалии, но это происходит уже не снаружи, а внутри. Если же становится известно о каких-либо слабостях в программном обеспечении межсетевого экрана, то их, несомненно, нужно немедленно устранять, а не наблюдать за тем, как их пытаются использовать.

Для того, чтобы система активного аудита, особенно распределенная, была практически полезной, необходимо обеспечить целостность анализируемой и передаваемой информации, а также целостность самой программной системы и ее живучесть в условиях отказа или компрометации отдельных компонентов (зачастую атака направляется сначала на средства безопасности, а уже потом — на прикладные компоненты). Ясно, что это проблема всех распределенных систем, и для ее решения служат сервисы взаимной аутентификации и контроля целостности (в том числе проверка подлинности источника данных). К сожалению, ситуация усложняется, если часть компонентов оказывается в неконтролируемой зоне (например, сенсоры в удаленном филиале). Мы ограничимся ссылками на работу по компьютерной иммунологии [12], на статью по живучести распределенных систем [13] и книгу [14], в которой в красках описывается применение воздействия на сенсоры в качестве мощного оружия дредноута Федерации.

3.3. Выявление злоумышленной активности

В том, что ты продаешь, вовсе не надо смыслить. Именно тогда продаешь всего успешней. Не видя изъянов, чувствуешь себя свободнее.

Э.М. Ремарк. «Тени в раю»

Под злоумышленной активностью мы понимаем как атаки (очевидно, противоречащие любой политике безопасности), так и действия, нарушающие политику безопасности конкретной организации путем злоупотребления имеющимися полномочиями. Разделение двух видов злоумышленной активности представляется нам целесообразным по той причине, что настройка на выявление атак может быть выполнена поставщиком системы активного аудита (атаки носят универсальный характер), в то время как политика безопасности (если, конечно, она есть) у каждой организации своя и настраиваться на нее заказчикам придется самим.

Для выявления злоумышленной активности пытались и пытаются использовать несколько универсальных технологий: экспертные системы, нейронные сети, сопоставление с образцом, конечные автоматы и т.п. Одной из первых и до сих пор самой употребительной остается технология обнаружения сигнатур злоумышленных действий. Идея состоит в том, чтобы каким-либо образом задать характеристики злоумышленного поведения (это и называется сигнатурами), а затем отслеживать поток событий в поисках соответствия с предопределенными образцами. Иногда сопоставление основывается на простом (применительно к активному аудиту — наивном) механизме регулярных выражений, известному всем по ОС Unix. В более серьезных разработках уже свыше десяти лет используются экспертные системы, опирающиеся на наборы правил, задающие более мощные языки.

Грубо можно считать, что экспертная система состоит из универсальной оболочки и наполнения в виде правил вывода, являющихся формализацией знаний о предметной области. В области активного аудита чаще всего используется оболочка P-BEST (Production-Based Expert System Toolset) (см. [15]). Ее мы и рассмотрим вместе с некоторыми сигнатурами атак, заимствованными из той же статьи [15].

```
rule [Bad_Login(#10;*):
   [e:event| event_type == login,
              return_code == 'BAD_PASSWORD]
==>
   [+bad_login| username = e.username,
                 hostname - e.hostname]
   [-|e]
   [!|printf("Bad login for user %s from host %s\n", e.username, e.hostname)]
]
```

Листинг 1. Пример правила на языке P-BEST.

Разумеется, мы не будем вдаваться в теорию и тонкости экспертных систем. Нас будут интересовать, в основном, вопросы эффективности и сопряжения с окружением (обычно управляющим). Отметим лишь, что P-BEST относится к категории систем прямого связывания, то есть она отправляется от известных фактов, сопоставляет их с записанными в правилах условиями и выводит новые факты до тех пор, пока не будет достигнута цель (в нашем случае — обнаружена злоумышленная активность).

Каждое правило состоит из двух частей: условия применимости (называемого также антецедентом) и правой части — консеквента. Когда очередное событие в отслеживаемом потоке делает истинным условие применимости некоторого правила, говорят, что правило «зажигается». Если консеквент содержит какие-либо действия, они выполняются (или помещаются в поле зрения компонента, принимающего решения о реагировании на злоумышленную активность).

В состав P-BEST входит компилятор pbcc, транслирующий правила вывода в функции языка C. После компиляции может быть получена либо самостоятельная экспертная система, либо набор библиотек, которые можно подключить к более широкому окружению. Для нас существенно, что язык P-BEST достаточно прост и интуитивно ясен, поэтому в принципе пользователи сами могут описывать на нем новые атаки и иные злоумышленные действия. Компиляция (в противовес интерпретации) правил позволяет получить эффективное решение, пригодное для работы в реальном масштабе времени. В состав антецедентов и консеквентов могут входить произвольные функции языка C. Это упрощает связь с окружением, программирование реакций и т.п.

Приведем пример простого правила, записанного на языке P-BEST (см. листинг 1). Оно обрабатывает неудачную попытку входа в систему. Предполагается, что ранее были описаны типы **`event`** и **`bad_login`** с соответствующими полями.

В первой строке, помимо названия правила, указан его приоритет (10), влияющий на порядок выполнения, а также дано разрешение на его многократное применение. Чтобы не случилось зацикливания, оператор «**`[-|e]`**» в консеквенте удаляет факт e из базы фактов, но предварительно в эту базу добавляет факт **`bad_login`**, который затем можно использовать, например, для подсчета числа неудачных попыток входа. Наконец, конструкция «**`!|`**» позволяет выполнять функции языка C. Разумеется, в реальных системах реакция должна быть более изощренной.

В качестве реального примера использования языка P-BEST рассмотрим правило, идентифицирующее атаки посредством переполнения буфера, резервируемого для хранения параметров (см. листинг 2). Подобные атаки используют ошибки в программном обеспечении, связанные с проверкой корректности параметров (точнее, с отсутствием или недостаточностью таких проверок). Если подходящим образом задать слишком длинные параметры некоторым утилитам, выполняющимся от имени суперпользователя (таким, например, как **`eject`** или **`fdformat`** в Solaris 2.5), можно выполнить в привилегированном режиме произвольную команду.

Приведенное правило рассчитано на модуль регистрации/аудита BSM в ОС Solaris. Идея выявления атак посредством переполнения буфера основана на анализе длины аргументов системных вызовов группы exec. Оказывается, размер учетной записи о «зловредном» exec составляет не менее 500 байт, в то время как в нормальных случаях он практически никогда не превышает 400.

В статье [15] приводятся и другие примеры. Например, набор для выявления атак на доступность «SYN flood» состоит из семи правил, самое длинное из которых насчитывает 12 строк. Это означает, что подобные наборы вполне реально разрабатывать самостоятельно.

Впрочем, выразительная сила языка правил для экспертных систем никогда не вызывала

```
rule[BSM_LONG_SUID_EXEC(*):
   [+e:bsm_event]
   [?|e.header_event_type == AUE_EXEC ||
      e.header_event_type == AUE_EXECVE]
   [?|e.subject.euid != e.subject.ruid]
   [?|e.header_size > 'NORMAL_LENGTH]
==>
   [!|printf("ALERT: buffer overrun attack on command %s\n", e.header_command)]
]
```

Листинг 2. Пример правила, выявляющего атаки посредством переполнения буфера параметров.

сомнений. Традиционной проблемой была эффективность функционирования. Согласно приведенным в статье [15] данным, на обработку регистрационного журнала размером 1.41 ГБ с числом записей 4.2 миллиона при 16 наборах правил на компьютере с процессором Pentium II (330 МГц) и операционной системой FreeBSD 2.2.6 потребовалось чуть больше 30 минут. Журнал был накоплен за пять суток (120 часов) работы. Значит, поиск сигнатур в данном случае отнимает менее 0.5% процессорного времени. Поскольку, как выяснилось, время обработки растет гораздо медленнее, чем первая степень числа правил, имеется масса резервов для увеличения количества сигнатур и усложнения выполняемых проверок.

Таким образом, подход, основанный на выявлении сигнатур злоумышленных действий средствами экспертных систем, оказывается вполне работоспособным со всех точек зрения.

Подчеркнем еще раз, что выразительная сила языка регулярных выражений для задания сигнатур, конечно, не является достаточной в силу возможности вариаций при проведении атак. Простая фрагментация IP-пакетов или смена подразумеваемых значений в зловредном коде на какие-то иные (например, изменение входного имени и/или пароля известной программы Back Orifice, см. [16]) способна обмануть систему активного аудита, использующую жесткие сигнатуры. Системы на основе регулярных выражений делать относительно несложно, но технологически они уже устарели, вне зависимости от занимаемой ими доли рынка.

Впрочем, справедливости ради следует отметить, что проблема устойчивости сигнатур по отношению к вариациям злоумышленных действий в большей или меньшей степени неприятна для любого подхода.

Но самой сложной проблемой для сигнатурного подхода является обнаружение ранее неизвестных атак. Выше мы указывали, что новые угрозы появляются практически каждый день. Бороться с ними можно двумя способами.

Во-первых, можно регулярно обновлять набор сигнатур. Здесь, помимо полноты, критически важной является частота обновлений. Сигнатуры новых атак должны предоставляться заказчикам на порядок быстрее, чем заплаты от производителей скомпрометированных аппаратных или программных продуктов. На практике это означает обновление в течение суток, но никак не раз в месяц. В противном случае системы активного аудита начинают напоминать фиговый листок, а не средство защиты от реальных угроз.

Во-вторых, можно (и нужно) сочетать сигнатурный подход с методами выявления аномальной активности, к рассмотрению которых мы и переходим. Атака или злоупотребление полномочиями — это почти всегда аномалия. Дело за малым — не пропустить ее и не поднимать слишком часто ложных тревог.

3.4. Выявление аномальной активности

Не забивайте себе этим голову, Росс.
Если во всех случайностях видеть проявление судьбы, нельзя будет и шагу ступить.
Э.М. Ремарк. «Тени в раю»

Для выявления аномальной активности было предложено довольно много методов (см. [17]): нейронные сети, экспертные системы, статистический подход. В свою очередь, статистический подход (он является темой нашего рассмотрения) можно подразделить на кластерный и факторный анализ, а также дискриминантный (классификационный) анализ. Не вдаваясь в детали, укажем, что буквальное применение этих методов не дает хороших результатов; необходимо учитывать специфику предметной области — активного аудита.

Статистический анализ (с учетом сделанных оговорок) представляется нам наиболее перспективным, отчасти «от противного», в силу недостатков, присущих другим подходам.

У нейронных сетей две основные проблемы:

- непонятность результатов: нейронная сеть принимает решение, но не объясняет, почему оно было принято;
- нехватка адекватного обучающего материала: невозможно создать базу всех типов аномалий.

Публикации с анонсами «почти работающих» нейронных сетей появлялись неоднократно, однако автору не приходилось читать о просто готовых и работающих системах.

Основной недостаток экспертных систем был указан выше — неумение выявлять (и, следовательно, отражать) неизвестные атаки.

У статистического подхода также есть проблемы:

- относительно высокая вероятность ложных тревог (нетипичность поведения не всегда означает злой умысел);
- плохая работа в случаях, когда действия пользователей не имеют определенного шаблона, когда с самого начала пользователи совершают злоумышленные действия (злоумышленные действия типичны), наконец, когда пользователь постепенно изменяет шаблон своего поведения в сторону злоумышленных действий.

Тем не менее, как показывает опыт, с этими проблемами можно бороться.

Выявление аномальной активности статистическими методами основывается на сравнении краткосрочного поведения с долгосрочным. Для этого измеряются значения некоторых параметров работы субъектов (пользователей, приложений, аппаратуры). Параметры могут отличаться по своей природе; можно выделить следующие группы:

- категориальные (измененные файлы, выполненные команды, номер порта и т.п.);
- числовые (процессорное время, объем памяти, количество просмотренных файлов, число переданных байт и т.п.);
- величины интенсивности (число событий в единицу времени);
- распределение событий (таких как доступ к файлам, вывод на печать и т.п.).

Алгоритмы анализа могут работать с разнородными значениями, а могут преобразовать все параметры к одному типу (например, разбив область значения на конечное число подобластей и рассматривая все параметры как категориальные). Выбор измеряемых характеристик работы — очень важный момент. С одной стороны, недостаточное число фиксируемых параметров может привести к неполноте описания поведения субъекта и к большому числу пропуска атак; с другой стороны, слишком большое число отслеживаемых характеристик потребует слишком большого объема памяти и замедлит работу алгоритма анализа.

Измерения параметров накапливаются и преобразуются в профили — описания работы субъектов. Суть преобразования множества результатов измерения в профили — сжатие информации. В результате от каждого параметра должно остаться лишь несколько значений статистических функций, содержащих необходимые для анализирующего алгоритма данные. Для того, чтобы профили адекватно описывали поведение субъекта, необходимо отбрасывать старые значения параметров при пересчете значений статистических функций. Для этого, как правило, используется один из двух методов:

- Метод скользящих окон — результаты измерений за некоторый промежуток времени (для долгосрочных профилей — несколько недель, для краткосрочных — несколько часов) сохраняются; при добавлении новых результатов старые отбрасываются. Основным недостатком метода скользящих окон является большой объем хранимой информации.
- Метод взвешенных сумм — при вычислении значений статистических функций более старые данные входят с меньшими весами (как правило, новые значения функций вычисляются по рекуррентной формуле, и необходимость хранения большого количества информации отпадает). Основным недостатком метода является более низкое качество описания поведения субъекта, чем в методе скользящих окон.

Итак, долгосрочные профили содержат в себе информацию о поведении субъектов за последние несколько недель; обычно они пересчитываются раз в сутки, когда загрузка системы минимальна. Краткосрочные профили содержат информацию о поведении за последние несколько часов или даже минут; они пересчитываются при поступлении новых результатов измерений.

Сравнение краткосрочных и долгосрочных профилей может производиться разными способами. Можно просто проверять, все ли краткосрочные значения попадают в доверительные интервалы, построенные по долгосрочному профилю. Однако в этом случае аномалии, распределенные по нескольким параметрам, могут остаться незамеченными. Поэтому предпочтительнее анализировать профили в совокуп-

ности. Далее, измеряемые характеристики, как правило, не являются независимыми, поэтому было бы желательным, чтобы влияние параметров на решение о типичности поведения было пропорционально степени их независимости.

В работе [18] рассматривается ряд сценариев сетевой активности и предлагаются эффективно работающие наборы параметров. Так, для сервисов типа SMTP или FTP целесообразно отслеживать категориальные характеристики: имена каталогов, к которым осуществляется доступ; протоколы, используемые для определенных портов; типы фиксируемых ошибок.

Отметим, что полезной числовой характеристикой является количество зафиксированных ошибок. При этом обнаруживается не только злоумышленное поведение, но и сбои и отказы аппаратуры и программ, что также можно считать нарушением информационной безопасности. Разумеется, целесообразно измерять и объем сетевого трафика. Аномальными являются отклонения в обе стороны (слишком большой трафик — сервис используют в злоумышленных целях, слишком маленький — нарушена доступность сервиса).

Применительно к сетевому трафику и некоторым другим событиям полезным классом величин оказывается интенсивность. Например, резкое нарастание попыток установления транспортных соединений может быть свидетельством SYN-атаки или сканирования портов.

Анализ распределения событий позволяет установить, как события влияют на те или иные значения. Например, выполнение команды cd в FTP-сеансе влияет на категориальную величину «каталоги», но не влияет на величины, ассоциированные с файлами. Если случилось обратное, значит, нормальная работа FTP-сервиса по каким-либо причинам нарушена. Вообще анализ распределения событий — эффективный способ выявления корреляций, в частности, между сигналами, поступающими на центральную консоль от подсистем активного аудита. Возможно, с точки зрения отдельных подсистем события выглядят не настолько подозрительными, чтобы поднимать тревогу, но совместный анализ распределений позволяет обнаружить скоординированную атаку.

Для успеха статистического подхода важен правильный выбор субъектов, поведение которых анализируется. На наш взгляд, целесообразно анализировать поведения сервисов или их компонентов (например, доступ анонимных пользователей к FTP-сервису). По сравнению с отдельными пользователями, поведение сервисов отличается большей стабильностью, да и для информационной безопасности организации важны именно сервисы. Совсем нет смысла анализировать сетевой трафик «вообще», его также нужно структурировать по типам поддерживаемых сервисов (плюс служебные моменты сетевого и транспортного уровней, такие как установление соединений).

Статистический подход является предметом интенсивных исследований, но уже сейчас он обладает достаточной зрелостью, используется в академических и коммерческих разработках. Можно ожидать, что со временем его позиции будут укрепляться. Во всяком случае, системы активного аудита, в которых статистический компонент отсутствует, не могут претендовать на полноту защитных функций.

3.5. Реагирование на подозрительные действия

После того, как обнаружена сигнатура злоумышленного действия или нетипичная активность, необходимо выбрать достойный ответ. По многим соображениям удобно, чтобы компонент реагирования содержал собственную логику, фильтруя сигналы тревоги и сопоставляя сообщения, поступающие от подсистем анализа. Для активного аудита одинаково опасны как пропуск атак (это значит, что не обеспечивается должной защиты), так и большое количество ложных тревог (это значит, что активный аудит быстро отключат).

При выборе реакции особенно важно определить первопричину проблем. Для сетевых систем это особенно сложно в силу возможности подделки адресов в пакетах. Данный пример показывает, что сильнодействующие средства, пытающиеся воздействовать на злоумышленника, сами могут стать косвенным способом проведения атак.

Предпочтительны более спокойные, но также достаточно эффективные меры, такие как блокирование злоумышленного сетевого трафика средствами межсетевого экранирования (ряд систем активного аудита умеют управлять конфигурацией экранов) или принудительное завершение сеанса работы пользователя. Конечно, и здесь остается опасность наказать невиновного, так что политика безопасности каждой организации должна определять, что важнее — не пропустить нарушение или не обидеть лояльного пользователя.

С точки зрения быстрого реагирования, традиционные меры, связанные с информированием администратора, не особенно эффективны. Они хороши в долгосрочном плане, для глобального анализа защищенности командой профессионалов. Здесь активный аудит смыкается с пассивным, обеспечивая сжатие регистраци-

онной информации и представление ее в виде, удобном для человека.

Разумная реакция на подозрительные действия может включать увеличение степени детализации протоколов и активизацию средств контроля целостности. В принципе, это пассивные меры, но они помогут понять причины и ход развития нарушения, так что человеку будет проще выбрать «меру пресечения».

Вероятно, в перспективе нормой станет взаимодействие с системами, через которые поступает подозрительный сетевой трафик. Это поможет пресечению злоумышленной активности и прослеживанию нарушителя. Некоторые подходы к данной проблеме мы рассмотрим ниже, в разделе «Стандарты в области активного аудита».

3.6. Требования к системам активного аудита

В этом пункте мы рассмотрим требования к системам активного аудита, существенные с точки зрения заказчиков.

На первое место следует поставить требование полноты. Это весьма емкое понятие, включающее в себя следующие аспекты:

- **Полнота отслеживания информационных потоков к сервисам**. Активный аудит должен охватывать все потоки всех сервисов. Это означает, что система активного аудита должна содержать сетевые и системные сенсоры, анализировать информацию на всех уровнях — от сетевого до прикладного. Очевидно, из рассматриваемого аспекта полноты вытекает требование расширяемости, поскольку ни один программный продукт не может быть изначально настроен на все сервисы.
- **Полнота спектра выявляемых атак и злоупотреблений полномочиями.** Данное требование означает не только то, что у системы должен быть достаточно мощный язык описания подозрительной активности (как атак, так и злоупотреблений полномочиями). Этот язык должен быть прост, чтобы заказчики могли производить настройку системы в соответствии со своей политикой безопасности. Поставщик системы активного аудита должен в кратчайшие сроки (порядка суток) передавать заказчику сигнатуры новых атак. Система должна уметь выявлять аномальную активность, чтобы справляться с заранее неизвестными способами нарушений.
- **Достаточная производительность.** Система активного аудита должна справляться с пиковыми нагрузками защищаемых сервисов. Пропуск даже одного сетевого пакета может дать злоумышленнику шанс на успешную атаку. Если известно, что система активного аудита обладает недостаточной производительностью, она может стать объектом атаки на доступность, на фоне которой будут развиваться другие виды нападения. Для локальных сетей стандартными стали скорости 100 Мбит/с. Это требует от системы активного аудита очень высокого качества реализации, мощной аппаратной поддержки. Если учесть, что защищаемые сервисы находятся в постоянном развитии, то станет понятно, что требование производительности одновременно является и требованием масштабируемости.

Помимо полноты, системы активного аудита должны удовлетворять следующим требованиям:

- **Минимум ложных тревог**. В абсолютном выражении допустимо не более одной ложной тревоги в час (лучше, если их будет еще на порядок меньше). При интенсивных потоках данных между сервисами и их клиентами подобное требование оказывается весьма жестким. Пусть, например, в секунду по контролируемому каналу проходит 1000 пакетов. За час пакетов будет 3 600 000. Можно предположить, что почти все они не являются злоумышленными. И только один раз система активного аудита имеет право принять «своего» за «чужого», то есть вероятность ложной тревоги должна составлять в данном случае не более $3 * 10^{-7}$.
- **Умение объяснять причину тревоги**. Выполнение этого требования во-первых, помогает отличить обоснованную тревогу от ложной, во-вторых, помогает определить первопричину инцидента, что важно для оценки его последствий и недопущения повторных нарушений. Даже если реагирование на нарушение производится в автоматическом режиме, должна оставаться возможность последующего разбора ситуации специалистами.
- **Интеграция с системой управления и другими сервисами безопасности**. Интеграция с системой управления имеет две стороны. Во-первых, сами средства активного аудита должны управляться (устанавливаться, конфигурироваться, контролироваться) наравне с другими инфраструктурными сервисами. Во-вторых, активный аудит может (и должен) поставлять данные в общую базу данных управления. Интеграция с сервисами безопасности необходима как для лучшего анализа ситуации (например, с привлечением средств кон-

троля целостности), так и для оперативного реагирования на нарушения (средствами приложений, операционных систем или межсетевых экранов).

- **Наличие технической возможности удаленного мониторинга информационной системы**. Это спорное требование, поскольку не все организации захотят оказаться под чьим-то «колпаком». Например, в США планы администрации Клинтона по мониторингу информационных систем федеральных организаций (см. [19]) натолкнулись на жесткое противодействие. Тем не менее, с технической точки зрения подобная мера вполне оправдана, поскольку большинство организаций не располагает квалифицированными специалистами по информационной безопасности. Отметим, впрочем, что удаленный мониторинг может быть использован и для бесспорных целей, таких как контроль из штаб-квартиры за работой удаленных отделений.

Сформулированные требования можно считать максималистскими. По-видимому, ни одна современная коммерческая система, ни один поставщик не удовлетворяют им в полной мере, однако, без их выполнения активный аудит превращается из серьезного оборонительного оружия в сигнализацию для отпугивания детей младшего школьного возраста. Захотят ли заказчики платить деньги за подобные игрушки? Нет, конечно, если только они достаточно разбираются в предмете.

Системы активного аудита принадлежат к области высоких технологий. У них развитая математическая база, продвинутая архитектура, они вобрали в себя знания по информационной безопасности. Мало кто из реселлеров понимает, как работает то, что они продают; им остается пересказывать рекламные буклеты производителей, где, конечно, все выглядит замечательно. Заказчики тоже не обязаны вдаваться в детали, но они должны знать, о чем спрашивать поставщиков. Не всегда те смогут ответить, но и молчание многое скажет заказчику.

4. Стандарты в области активного аудита

Активный аудит — относительно новая область коммерческой деятельности, однако, проблемы совместимости, согласованной работы различных систем, разумеется, уже дают о себе знать. Начинают формироваться стандарты, которые можно назвать внутренними. Они помогают взаимодействовать между собой компонентам систем активного аудита и системам в целом. Мы кратко опишем две инициативы. Одна исходит от Интернет-сообщества, другая — от академических кругов.

4.1. Обмен данными о подозрительной активности

Многие атаки на информационные системы носят распределенный характер. При этом разные средства активного аудита видят один и тот же инцидент с разных точек зрения. Несомненно, совместный, многоаспектный анализ полезен для прослеживания злоумышленников, определения причин и масштабов инцидентов. Разделение информации о подозрительной активности является главным направлением работ недавно созданной в рамках Тематической группы по технологии Интернет (Internet Engineering Task Force, IETF) Рабочей группы по обнаружению вторжений (Intrusion Detection Working Group, IDWG).

В июне 1999 года появился первый (на момент написания статьи — единственный) проект группы — «Требования к формату обмена данными о подозрительной активности» [20]. Это «мета-стандарт», выдвигающий довольно общие требования к будущим рекомендациям группы; тем не менее, он представляет несомненный интерес.

Группе IDWG предстоит специфицировать формат и процедуры разделения данных между системами выявления подозрительной активности, реагирования и управления. Для формата уже выбрано название, как это часто бывает, весьма неудачное: Intrusion Detection Exchange Format (IDEF). (Специалисты по технологии программирования знают, что аббревиатура IDEF уже давно занята.) Предполагается, что автоматизированные системы активного аудита будут использовать формат IDEF при формировании сообщений о подозрительной активности. На самом деле требования [20] разрабатывались, в первую очередь, в расчете на взаимодействие между анализирующим компонентом и компонентом реагирования, происходящее по протоколу TCP/IP.

Прежде всего, в [20] формулируются общетехнические требования, призванные сделать формат IDEF универсальным и долгоживущим.

IDEF должен поддерживать все механизмы обнаружения подозрительной активности. Он должен быть рассчитан на IPv6, содержать все необходимое для интернационализации/локализации, поддерживать фильтрацию и агрегирование сообщений компонентом реагирования, их надежную доставку (в том числе через межсетевой экран без внесения в конфигурацию последнего изменений, способных ослабить периметр безопасности).

Разумеется, формат IDEF должен поддерживать взаимную аутентификацию общающихся сторон, неотказуемость от факта передачи, а также целостность и конфиденциальность потока сообщений.

В сообщениях формата IDEF должны содержаться дата и время подозрительных событий и, если возможно, дата и время атаки. Естественно, оговаривается, что формат даты должен быть свободен от Проблемы 2000 и аналогичных сложностей. Специфицируется присутствие в сообщениях списка сенсоров, зафиксировавших подозрительное событие.

Если анализатор сам принял ответные меры, в IDEF-сообщениях должна быть информация об этом. Если анализатор может оценить последствия зафиксированной атаки, он также обязан сообщить об этом.

Формат IDEF должен поддерживать информацию о производителе системы активного аудита, сгенерировавшей сообщение, а также расширения, специфичные для конкретной системы.

Предполагается, что будет утвержден список стандартных атак и методов их проведения. Если анализатор может идентифицировать атаку и используемый метод, он должен включить соответствующую информацию в IDEF-сообщение. Если атака является нестандартной, ее имя может быть специфичным для производителя системы активного аудита.

В сообщениях могут содержаться идентификаторы источника и цели атаки. Если атака имеет сетевой характер, в качестве идентификаторов могут использоваться IP-адреса. Для системных и прикладных атак идентификаторы источника/цели пока не ясны.

Формат IDEF должен допускать включение в сообщения дополнительной информации, ассоциированной с подозрительным событием. В частности, в сообщениях должно быть предусмотрено поле для размещения рекомендаций какого-либо авторитетного органа, такого как CERT.

Будем надеяться, что выполнение сформулированных требований не заставит себя долго ждать, и уже в этом, 1999 году, мы увидим спецификации формата сообщений и процедур обмена.

4.2. Общий каркас систем активного аудита

Общий каркас систем активного аудита (Common Intrusion Detection Framework, CIDF, см. [21]) разрабатывается группой исследовательских организаций, финансируемых агентством DARPA и работающих в области выявления подозрительной активности. Впрочем, присоединиться к группе может любой желающий.

Цель создания общего каркаса близка к исходным посылкам группы IDWG (см. предыдущий пункт) — обеспечить интероперабельность и разделение информации различными системами активного аудита и их компонентами, максимизировать повторное использование последних в различных контекстах. В сходстве целей нет ничего удивительного, поскольку именно участники группы CIDF стали инициаторами организации группы IDWG, хотя теперь последняя живет своей, вообще говоря, независимой жизнью.

В рамках CIDF разработан язык описания подозрительной активности и способ кодирова-

```
(Delete
    (Context
        (HostName 'main.strange.com')
        (Time '23:55:12 Aug 11 1999')
    )
    (Initiator
        (UserName 'root')
    )
    (Source
        (FileName '/etc/passwd')
    )
)
```

Листинг 3. Пример S-выражения языка CIDF.

ния информации о подозрительных событиях. Язык приспособлен для описания по крайней мере трех видов сообщений:

- «сырой» информации о событиях (например, записей регистрационного журнала или сетевых пакетов);
- результатов анализа (таких как выявленные аномалии или атаки);
- рекомендованных реакций (прервать какую-либо активность или изменить конфигурацию защитных средств).

Кроме того, на языке могут быть описаны следующие сущности:

- связи между событиями (например, причинно-следственные);
- роли объектов в событиях (например, объект инициировал событие);
- свойства объектов;
- связи между объектами.

По внешнему виду язык CIDF является лисподобным. Его основу составляют так называемые S-выражения, первым элементом которых должен быть семантический идентификатор, определяющий смысл последующих элементов. В статье [21] среди прочих приводится пример S-выражения, воспроизведенный нами на листинге 3 с небольшими изменениями.

Данное выражение означает, что в указанное время пользователь `root` удалил файл `/etc/passwd` на компьютере `main.strange.com`. Семантические идентификаторы задают действия (`Delete`) и роли (`Context`, `Initiator` и т.п.), выполняемые объектами. В результате становится понятно, что, кто, где и когда сделал.

Для организации взаимодействия между компонентами в каркасе CIDF предлагается использовать службу каталогов (LDAP). Компоненты регистрируются и афишируют виды выражений, которые они отправляют или воспринимают. Разумеется, в каталоге может быть и другая информация, например, сертификаты в стандарте X.509 и т.п.

На момент написания данной статьи судьба спецификаций CIDF представляется неясной. С одной стороны, в них предложены вполне разумные идеи. С другой стороны, какой-либо поддержки со стороны производителей коммерческих систем у CIDF нет (возможно, потому, что производители еще не доросли до стандартов). Вероятно, центр активности переместится в группу IDWG и инициатива CIDF постепенно угаснет. Однако не вызывает сомнений, что в ближайший год ядро стандартов в области активного аудита так или иначе сформируется, что, несомненно, в перспективе облегчит заказчикам построение интегрированных систем безопасности и управления.

5. Примеры систем активного аудита

В этом разделе мы рассмотрим системы активного аудита, наиболее интересные, на наш взгляд, с точки зрения архитектуры или реализованных в них идей. Мы не собираемся сравнивать и как-либо ранжировать подобные системы; занятие это рискованное и неблагодарное. Нам важно понять, какие идеи и каким образом реализуются, и что это дает. Тем, кто желает ознакомиться с перечнем и основными свойствами известных систем активного аудита, мы рекомендуем в качестве отправной точки аннотированный список [22], а также сборник ответов [16].

5.1. Система EMERALD

Система EMERALD (см., например, [23]) по сути является старейшей разработкой в области активного аудита, так как она вобрала в себя опыт более ранних систем — IDES и NIDES, созданных в Лаборатории информатики Стэнфордского исследовательского института (Stanford Research Institute, ныне известен как SRI International) по контракту с DARPA.

EMERALD расшифровывается как Event Monitoring Enabling Responses to Anomalous Live Disturbances — мониторинг событий, допускающий реакцию на аномалии и нарушения. EMERALD включает в себя все компоненты и архитектурные решения, необходимые для систем активного аудита, оказываясь тем самым не только старейшей, но и самой полной разработкой как среди исследовательских, так и среди коммерческих систем.

Строго говоря, EMERALD является не готовым продуктом, а программной средой, которая строится по модульному принципу. Основным «кирпичиком» служит монитор (см. рис. 6). Каждый монитор включает в себя компонент распознавания сигнатур злоумышленных действий, компонент выявления аномальной активности, решатель, выбирающий способ реагирования на нарушения, а также описание контролируемого объекта. Каждый монитор настраивается по описанию и следит за своим объектом. Мониторы распределяются по информационной системе, образуя иерархию. Отметим, что контролируемые объекты могут иметь как системную, так и сетевую природу. Таким образом, совокупность мониторов может покрыть «всех и каждого». Отметим также, что в иерархию могут включаться не только свои, но и чужие компоненты, разработанные другими производителями.

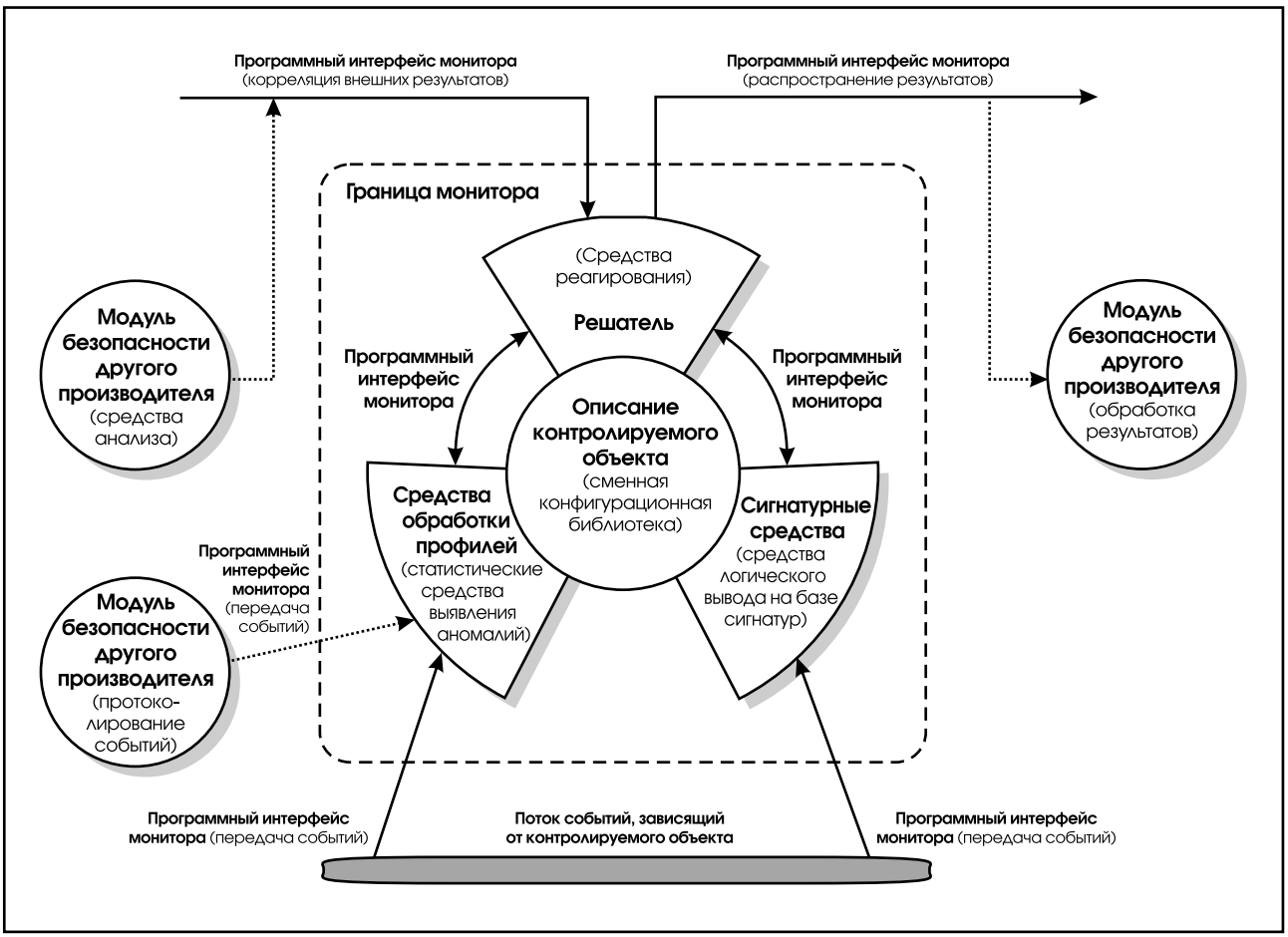

Рис. 6. Модуль системы EMERALD и его возможные связи.

В общем случае мониторы системы EMERALD развертываются динамически, после чего в реальном времени контролируют поведение инфраструктурных и/или прикладных сервисов. Данные для анализа могут собираться как «пассивным» чтением регистрационных журналов или сетевых пакетов, так и с помощью активных проб. Результаты анализа могут направляться в асинхронном режиме другим мониторам.

По сути, в разделе «Методы проведения активного аудита» мы уже рассмотрели архитектурные и реализационные решения, принятые в системе EMERALD. Для распознавания сигнатур злоумышленных действий используется экспертная система P-BEST, а выявление аномальной активности основано на применении четырех классов величин (категориальных, непрерывных, показателей интенсивности, распределениях). Статистическому анализу подвергается поведение не пользователей, а сервисов. Профили сервисов существенно меньше и они гораздо стабильнее, чем у пользователей. В результате удалось заметно снизить ошибки первого и второго рода, то есть пропуск нарушений политики безопасности и возбуждение ложных тревог.

В основе своей монитор не зависит от отслеживаемого объекта. Все специфическое вынесено в описание объекта, служащее для настройки подключаемых библиотек. Настраиваются такие методы, как сбор регистрационной информации, реагирование, а также аналитические параметры анализа, список соседей, с которыми нужно обмениваться сигналами тревоги и т.п.

EMERALD не навязывает определенной архитектуры. Можно выстроить совокупность слабосвязанных мониторов с «легковесным» локальным анализом или же жесткую иерархию с мощным централизованным анализом. Можно делать акцент на сетевых или системных сенсорах.

Разумеется, в среде EMERALD изначально существуют описания для элементов инфраструктуры (маршрутизаторы, межсетевые экраны) и прикладных сервисов (FTP, SMTP, HTTP и т.д.). Это означает, что, наряду с гибкостью и расширяемостью, EMERALD в достаточной степени удобен для быстрого развертывания в типичной информационной системе.

Одной из важнейших новаций системы EMERALD является корреляционный анализ сигналов тревоги, поступающих от разных мониторов. Такой анализ проводится по четырем категориям:

- выявление общих характеристик;
- исследование одного события с разных точек зрения;
- выявление связей между сигналами тревоги;
- выявление тренда (детерминированной составляющей).

Корреляционный анализ остается предметом исследования. Вероятно, это основное направление развития системы EMERALD.

Разработчики EMERALD планируют обеспечить следование спецификациям IDEF и CIDF. Разумный выбор архитектуры сделал эту задачу относительно несложной.

По мнению разработчиков, результаты, полученные при создании системы EMERALD, выглядят обнадеживающими. EMERALD годится не только для активного аудита, но и для решения других задач информационной безопасности и управления (например, поддержания высокой доступности или анализа поведения сети). Иерархическая организация мониторов и корреляционный анализ помогают выявлять скоординированные, распределенные атаки. Система EMERALD производит очень сильное впечатление.

5.2. Система NFR

Система NFR (Network Flight Recorder), как и EMERALD, привлекает, прежде всего, архитектурной и технологической правильностью. В подобной правильности нет ничего удивительного, поскольку руководителем разработки является Маркус Ранум (Marcus J. Ranum), видный специалист по информационной безопасности.

NFR относится к числу сетевых систем, существующих в виде свободно распространяемого инструментария и коммерчески «упакованного» продукта NFR Intrusion Detection Appliance (на момент написания данной статьи самая свежая версия имела номер 3.0). С внешней точки зрения NFR представляет собой либо одну станцию, осуществляющую мониторинг сегмента сети, к которому она подключена, либо совокупность таких станций с центральной управляющей консолью. Однако наиболее интересна не внешняя, а внутренняя архитектура NFR, превосходно описанная в статье [24].

Строго говоря, NFR — это нечто большее, чем система выявления подозрительной сетевой активности. Правильнее рассматривать ее как компонент сетевого управления, одним из аспектов которого является борьба с нарушениями политики безопасности (равно как и со сбоями и отказами оборудования и программного обеспечения).

Основные компоненты внутренней архитектуры NFR показаны на рис. 7. Один или несколько сетевых сенсоров (packet suckers в терминологии NFR) поставляют данные решателю, который эти данные фильтрует, реассемблирует потоки, при обнаружении нарушений реагирует на них, а также передает информацию поддерживающему сервису для сохранения с последующей статистической обработкой и обслуживанием запросов. Поддерживающий сервис может также просматривать переданную ему информацию на предмет выявления сигнатур злоумышленных действий.

Разумеется, для всех стыков определены программные интерфейсы, так что возможна, например, смена или добавление сенсора или поддерживающего сервиса. «Отвязывание» поддерживающего сервиса от сбора и первичного анализа регистрационной информации позволяет распределять нагрузку, чтобы сложная обработка не тормозила процессы, от которых требуется работа в реальном масштабе времени.

Ядром NFR является решатель, а основой решателя — язык описания фильтров, который называется N. Это универсальный язык программирования, содержащий переменные с об-

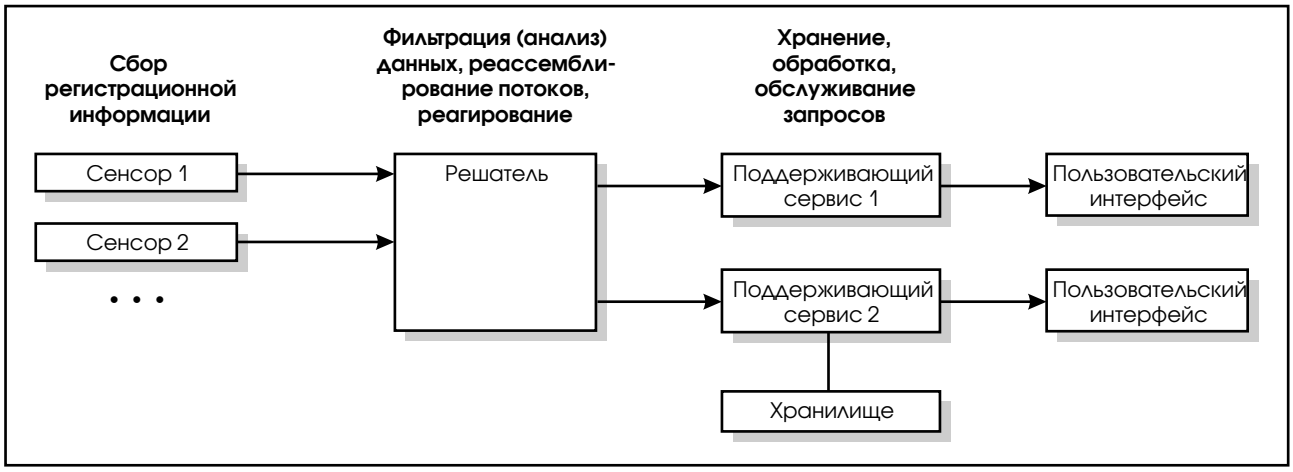

Рис. 7. Основные элементы архитектуры NFR.

```
filter server tcp (client, port: 80, start: "GET ", stop: " ") {
    record ip.src, ip.dst, tcp.sport, tcp.dport,
    tcp.bytes to urlRecorder;
}
```

Листинг 4. Фильтр на языке N, фиксирующий запрашиваемые пользователем локаторы ресурсов.

ластями видимости, списочные типы данных, управляющие структуры, процедуры. Кроме того, в N есть специфические типы данных, такие как IP-адрес. Любопытно отметить, что под значения разного рода счетчиков отводится по 64 разряда, что освобождает от проблем переполнения даже в больших сетях.

N — интерпретируемый язык. Программы, написанные на N, переводятся в байт-коды для простой стековой машины. Такие программы (и, следовательно, фильтры) оказываются весьма компактными. Что касается скорости интерпретации, то при достаточно высоком уровне базовых операций она оказывается не намного ниже, чем при выполнении скомпилированной программы. Кроме того, применяемый при интерпретации N-программ механизм ленивых вычислений позволяет избежать лишних операций, обычно сопутствующих проверке сложных условий.

В N заложены знания о структуре сетевых пакетов и протоколах более высоких уровней. Например, допустимы обращения вида ip.src, tcp.hdr или syslog.message. Возможно и обращение к произвольным частям пакетов. В принципе, на N можно написать интерпретатор любого прикладного протокола.

На листинге 4 приведен пример совсем простого фильтра, выбирающего запрашиваемые клиентом по протоколу HTTP локаторы ресурсов.

Этот фильтр анализирует TCP-соединения с серверным портом 80, ищет в потоке данных цепочку символов «GET «, записывает все от места совпадения до пробела в поле tcp.bytes (предполагается, что это и будет URL), после чего отправляет поддерживающему сервису исходные и целевые IP-адреса и номера TCP-портов, а также выявленный URL.

В данном случае разыскиваемый шаблон весьма прост. Подчеркнем, что язык N позволяет сделать его сколь угодно сложным.

Программы на N, поддерживающий сервис, интерпретатор могут генерировать сигналы тревоги, для обработки которых существует специальная программа, работающая в фоновом режиме. Эта программа на основе ассоциированной информации определяет дальнейший маршрут и приоритет сигналов тревоги.

NFR не является универсальной системой активного аудита, но представляет несомненный интерес, прежде всего, как хорошо сделанный строительный блок, который можно установить в управляющую среду, объединить со средствами выявления подозрительной активности на хостах и т.п. Язык N обладает достаточной мощностью и для записи сигнатур атак с учетом возможных вариаций, и для выражения сетевых аспектов политики безопасности организации. Правда, остается открытым вопрос об эффективности функционирования, от ответа на который разработчики предпочитают уходить, ссылаясь на зависимость от сложности заданных фильтров (см. [7]). То, что в качестве рекомендуемой конфигурации для NFR Intrusion Detection Appliance выбран компьютер с процессором Intel Pentium II 400 МГц и ОЗУ 256 МБ (см. [25]), вероятно, свидетельствует о наличии проблем с эффективностью. Впрочем, как с философским спокойствием говорится в финале известного фильма, «у каждого свои недостатки».

6. О результатах тестирования систем активного аудита

Тестировать и оценивать системы активного аудита трудно. Во-первых, не ясно, как составить реалистичную смесь лояльных и злоумышленных действий и видоизменять ее при появлении новых угроз. Во-вторых, подобную смесь не так просто «подать» в реальном времени в распределенную систему, в сеть и на хосты, обеспечивая при этом воспроизводимость результатов. Возможно, в силу перечисленных трудностей данной теме посвящено весьма небольшое число работ, в то время как важность проблемы трудно переоценить. Действительно, что же получает заказчик системы активного аудита? Каков процент «раскрываемости» злоумышленных действий? Какова предполагаемая частота ложных тревог? Какую нагрузку выдерживает система? Проще говоря, окупаются ли затраты на выявление подозрительной активности? Обычно поставщики не затрудняют себя ответами на подобные вопросы.

К счастью, иного мнения придерживаются в Управлении перспективных исследований и разработок Министерства обороны США

(Defence Advanced Research Projects Agency, DARPA), финансирующем более двадцати (!) проектов в области активного аудита. Там решили понять, каких результатов добились их «подопечные», и поручили Исследовательской лаборатории ВВС США (Air Force Research Laboratory, AFRL, кстати сказать, курирующей свыше 10 миллионов казенных долларов, вложенных в данное направление) разработать тестовую архитектуру и процедуру оценки систем активного аудита. Каждые полгода лаборатория AFRL должна публиковать полученные результаты.

Пока проведено одно тестирование и его нельзя считать всеобъемлющим, но результаты, приведенные в статье [26], на наш взгляд, представляют исключительный интерес.

Прежде всего, в AFRL создали тестовую конфигурацию и соответствующее программное обеспечение. За образец была взята типичная для военных организаций сеть городского масштаба (MAN). На рис. 8(а) приведена логическая, а на рис. 8(б) — физическая структура тестовой сети. Имитация присутствия дополнительных логических компонентов осуществляется программными средствами.

Важно отметить, что имитируются как внешние, так и внутренние атаки (на рис. 8(б) присутствуют два генератора трафика, каждый из которых видится остальным узлам как множество хостов, соответственно, внешних и внутренних). Очень часто основное внимание служб безопасности сосредоточено на внешних подключениях, что методически неверно. Внутренние злоумышленники гораздо опаснее внешних.

Для тестирования был заготовлен четырехчасовой трафик, включающий типичную смесь протоколов: HTTP (66%), SMTP (13%) и т.д. На этом фоне проводилось 30 атак, которые грубо можно примерно поровну разделить на четыре категории:

- разведка (сканирование портов, ping);
- атаки на доступность (в данном случае направлены против отдельных хостов, а не против сети в целом: SYN и др., атака на Apache);
- атаки с целью получения привилегий суперпользователя (в данном случае использовалось только переполнение разного рода буферов);
- внешние атаки (использовались слабости в конфигурации сетевых сервисов).

Все атаки (в том числе получение привилегий суперпользователя) проводились по сети,

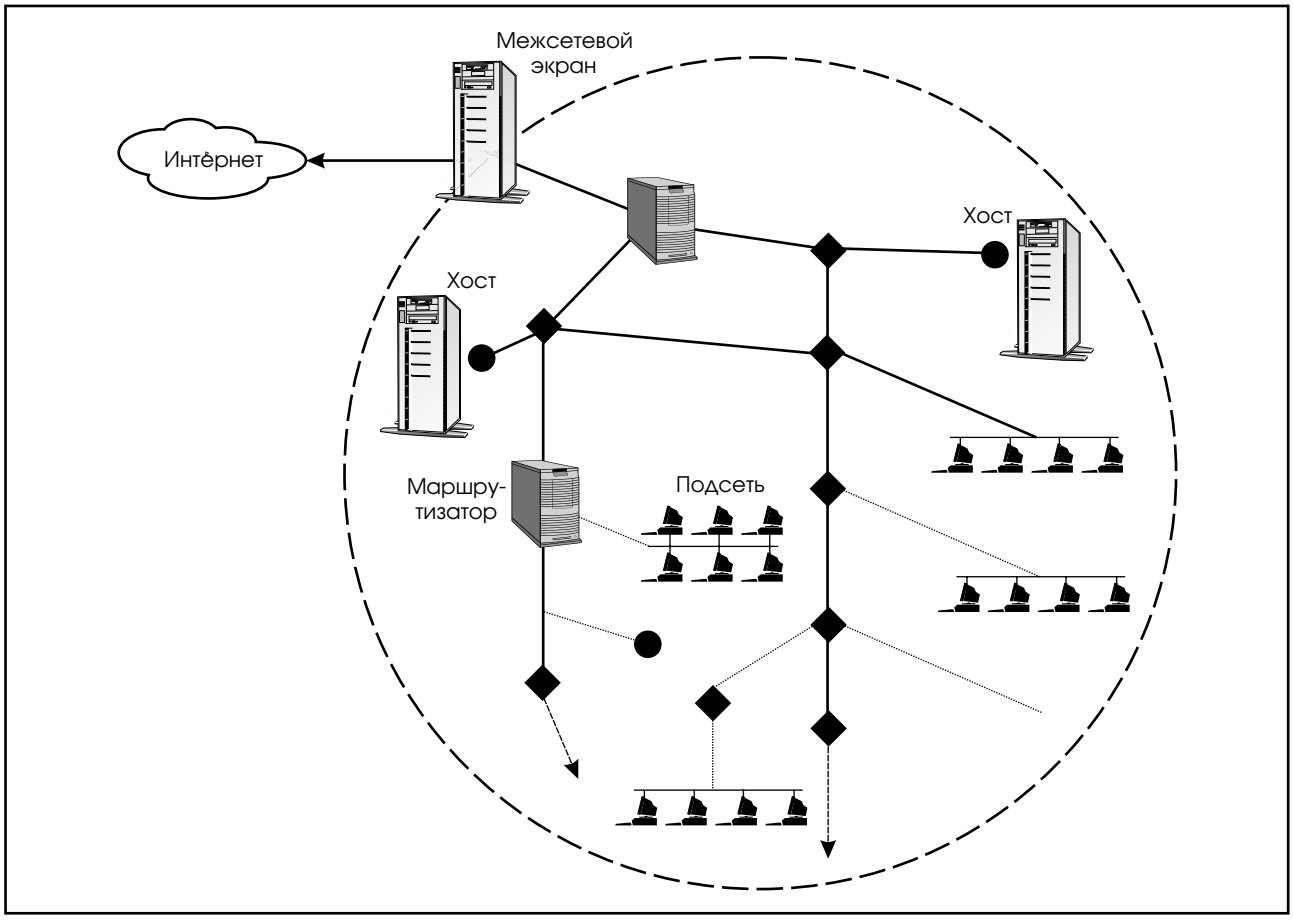

Рис. 8а. Логическая структура тестовой сети лаборатории AFRL.

чтобы в принципе их можно было обнаружить путем анализа перехваченных сетевых пакетов.

Фактически в тесте проверялись четыре системы активного аудита: одна коммерческая из числа широко используемых в военных организациях, а также три наиболее продвинутые разработки, финансируемые DARPA. Названия систем в статье [26] не приводятся, что, на наш взгляд, не имеет большого значения, поскольку тестировалось лучшее из имеющегося.

Все тестируемые системы использовали сигнатурный подход. Коммерческая система была чисто сетевой, с поиском в сетевых пакетах определенных цепочек байт; ее поместили у межсетевого экрана, как обычно и поступают в военных организациях. Одна исследовательская система включала сетевые и хостовые компоненты, две другие были чисто хостовыми. Если какая-то система не могла видеть часть атак, то считалось, что это ее проблемы (как, впрочем, и проблемы тех, кто подобные системы использует в меру своей квалификации и финансовых возможностей).

По результатам тестирования вычислялись два показателя: процент ложных тревог (по отношению к общему числу сеансов сетевого взаимодействия) и процент обнаруженных атак (разумеется, чтобы не вносить помех, реакция на атаки была отключена). У коммерческой системы можно было варьировать коэффициент подозрительности, повышая «раскрываемость» вместе с числом ложных тревог; исследовательские системы действовали безусловно: либо атака выявляется, либо нет.

Коммерческая система при доле ложных тревог в 1% (дальше повышать ее, очевидно, бессмысленно) выявила приблизительно 12% атак. У исследовательских систем доля ложных тревог оказалась заметно меньше: 0% у одной и менее 0.1% у двух других. Доля обнаруженных атак составила, соответственно, примерно 14%, 18% и 25%. Даже если поставить все четыре системы и сложить приходящиеся на них проценты, до сотни окажется далековато...

Кроме количественных, обращают на себя внимание следующие качественные результаты:

- в рамках сигнатурного подхода можно добиться минимизации числа ложных тревог;
- сетевые системы активного аудита неэффективны при распознавании «хостовых» атак (атак с целью получения привилегий суперпользователя);
- путем ограничения темпа и масштаба сканирования можно скрыть разведывательные

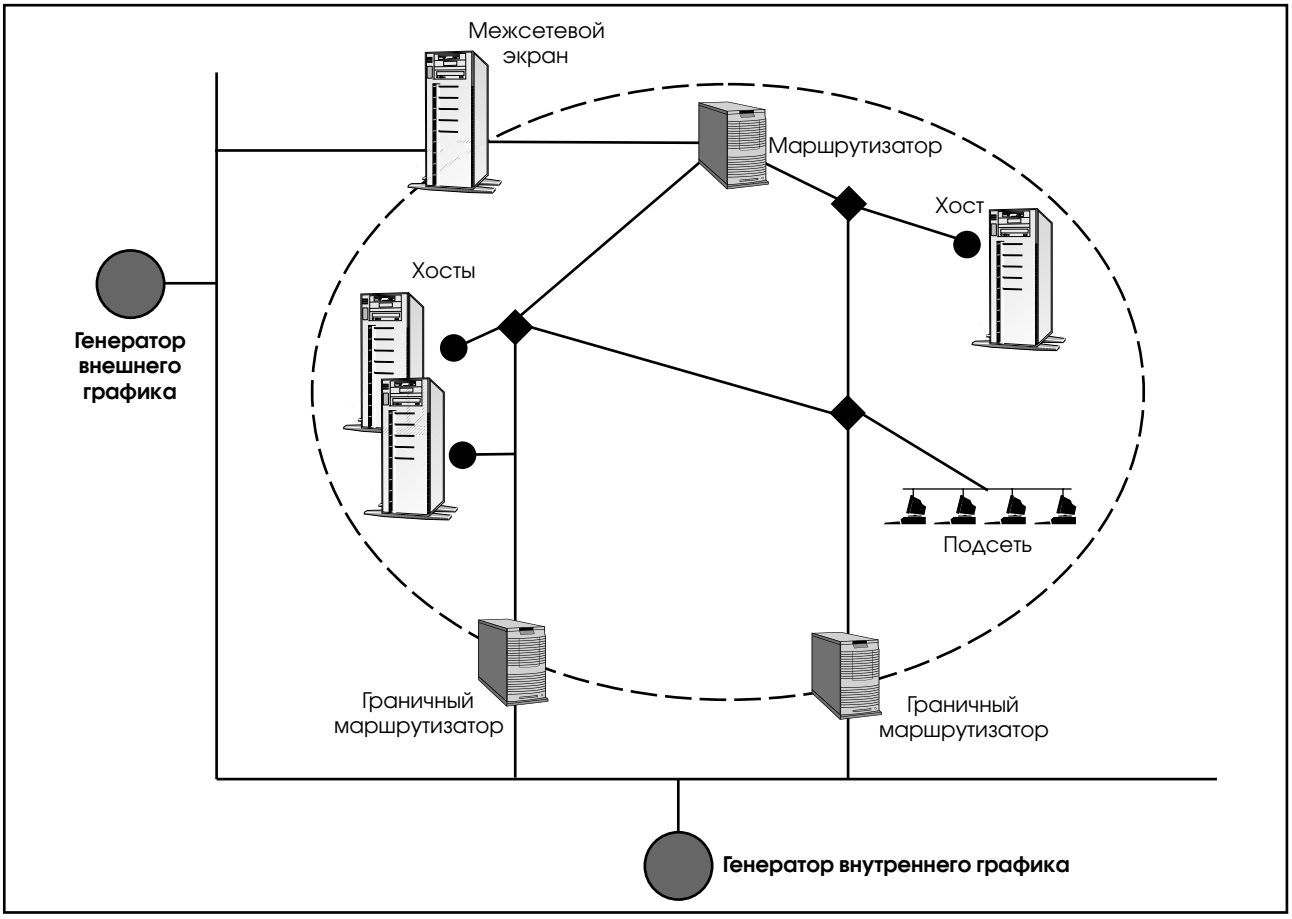

Рис. 8б. Физическая структура тестовой сети лаборатории AFRL.

действия, добывая при этом необходимую информацию;

- сигнатурный подход неэффективен для распознавания неизвестных атак;
- подход на основе поиска в сетевых пакетах заданных регулярных выражений (типичный для коммерческих систем, используемых американскими военными), ведет к большому числу ложных тревог и оставляет необнаруженными большую часть атак.

Еще раз подчеркнем, что выводы, сделанные после первого тестирования, не претендуют на окончательность. Нужно увеличивать число атак, число тестируемых систем, варьировать способы проведения атак (кстати сказать, для начала системы активного аудита были поставлены в тепличные условия: трафик не шифровался, с большинством планируемых атак разработчики исследовательских систем имели возможность ознакомиться заранее). С другой стороны, под давлением разработчиков какие-то приемы тестирования могут быть отвергнуты как «нечестные». Тем не менее, приведенные результаты настолько далеки от идеала, что едва ли «дыру» можно залатать добавлением подсистем выявления аномальной активности. Впрочем, подождем следующих результатов. Тогда прояснится не только текущая ситуация, но и тенденции.

7. Заключение

Итак, жизнь продолжается.
Она может быть страшной или прекрасной
в зависимости от того, как на нее смотреть.
Проще было считать ее прекрасной.

Э.М. Ремарк. «Тени в раю»

Активный аудит, в зависимости от точки зрения, можно считать и весьма зрелой, и только формирующейся областью информационных технологий.

С одной стороны, исследования по выявлению подозрительной активности ведутся давно, в процессе этих исследований были получены интересные математические и программистские результаты. Исследования носят комплексный характер, они направлены на создание эффективных, гибких, расширяемых, масштабируемых систем, способных стать надежным защитным рубежом в корпоративных сетях произвольного размера. На наш взгляд, почти все необходимые концептуальные и архитектурные решения уже найдены; начинается фаза инженерной «доводки». Наиболее неисследованной областью остается обнаружение низкоскоростных, скоординированных атак из нескольких источников.

С другой стороны, коммерческие системы активного аудита появились относительно недавно и соответствующий рынок пока невелик. К сожалению, разработчики коммерческих систем предпочли «искать под фонарем», взяв на вооружение, прежде всего, звучный термин «обнаружение вторжений», но ограничившись применением самых простых методов. Часть систем является просто перелицованными сканерами безопасности, что, конечно, экономически оправдано с точки зрения производителя, но едва ли благоприятно сказывается на качестве продукта. Слишком много вариантов атак пропускается, слишком много ложных тревог генерируется, слишком много времени проходит от появления новой атаки до установки у заказчика соответствующих сигнатур.

Реальность, однако, состоит в том, что при любом взгляде на проблему выявления подозрительной активности подобные системы, несомненно, нужны. Если на самом деле обнаруживается лишь 4% атак, то это даже меньше, чем видимая часть айсберга, а ведь и сейчас статистика нарушений информационной безопасности выглядит угрожающе. Нужно находить (и наказывать) злоумышленников, нужно что-то делать с оставшимися 96% нарушений, и основная надежда связывается именно с активным аудитом (если, конечно, не считать кардинального решения в виде революции в технологии создания больших информационно-безопасных систем).

На наш взгляд, должно пройти еще 3-5 лет, прежде чем коммерчески доступные, недорогие системы активного аудита станут реальным защитным средством, пригодным для эффективной эксплуатации массовым заказчиком, но уже сейчас их можно использовать для повышения безопасности критически важных сервисов или отдельных участков сети. Целесообразно сочетать их с более простыми средствами контроля целостности, автоматизируя реакцию на выявленные нарушения. Возможно, части организаций следует подумать о мониторинге своей информационной системы с привлечением профессионалов.

Работы в области активного аудита ведутся исключительно интенсивно. Они просто не могут не дать положительного результата. Нужно только немного подождать.

8. Литература

1. Cyber attacks rise from outside and inside corporations. — Computer Security Institute, 1999. http://www.gocsi.com/prelea990301.htm.
2. Global Security Survey: Virus Attack. — InformationWeek от 12 июля 1999 года в изло-

жении Edupage (July 19, 1999). http://listserv.educase.edu/archives/edupage.html.

3. National Infrastructure Protection Center CyberNotes #15-99. — NIPC, 1999. http://www.fbi.gov/nipc/cyberissue15.pdf.
4. Галатенко В. Современная трактовка сервисов безопасности. — Jet Info, 1999, 5.
5. Information Security: Computer Attacks at Department of Defense Pose Increasing Risks. — General Accounting Office, Chapter Report, 05/22/96, GAO/AIMD-96-84. http://www.nswc.navy.mil/ISSEC/Docs/GAO_AIMD-96-84.html.
6. Столяров М., Трифаленков И. На пути к управляемым информационным системам. — Jet Info, 1999, 3.
7. Power R. CSI Roundtable: Experts discuss present and future intrusion detection systems. — Computer Security Journal, Vol. XIV, #1. http://www.gocsi.com/roundtable.htm.
8. Denning D. An Intrusion-Detection Model. — IEEE Transactions on Software Engineering, February 1987/Vol. SE-13, No. 2, pp. 222-232.
9. Bace R. An Introduction to Intrusion Detection Assessment. — ICSA, 1999. http://www.icsa.net/services/consortia/intrusion/educational_material.shtml.
10. Bass T. Intrusion Detection Systems & Multisensor Data Fusion: Creating Cyberspace Situational Awareness. — Communicaions of the ACM, accepted for publication (draft). http://www.valuerocket.com/papers/acm.fusion.ids.ps.
11. Goan T. A Cop on the Beat: Collecting and Appraising Intrusion Evidence. — Communicaions of the ACM, July 1999/Vol. 42, No. 7, pp. 46-52. http://www.acm.org/pubs/articles/journals/cacm/1999-42-7/p46-goan/.
12. Stillerman M., Marceau C., Stillman M. Intrusion Detection for Distributed Applications. — Communicaions of the ACM, July 1999/Vol. 42, No. 7, pp. 62-69. http://www.acm.org/pubs/articles/journals/cacm/1999-42-7/p62-stilleman/.
13. Ghosh A., Voas J. Inoculating Software for Survivability. — Communicaions of the ACM, July 1999/Vol. 42, No. 7, pp. 38-44. http://www.acm.org/pubs/articles/journals/cacm/1999-42-7/p38-ghosh/.
14. Кэри Д. Дредноут (пер с англ.). — Смоленск: Русич, 1996.
15. Lindqvist U., Porras P. Detecting Computer and Network Misuse Through the Production-Based Expert System Toolset (P-BEST). — Proceedings of the 1999 IEEE Symposium on Security and Privacy, Oakland, California, May 9-12, 1999.
16. Graham R. FAQ: Network Intrusion Detection Systems. — Version 0.5.2, July 17, 1999. http://www.robertgraham.com/pubs/network-intrusion-detection.html.
17. Галатенко А. О применении методов теории вероятностей для решения задач информационной безопасности. — М.: НИИСИ РАН, 1999.
18. Porras P., Valdes A. Live Traffic Analysis of TCP/IP Gateways. — Proceedings of the 1998 ISOC Symposium on Network and Distributed Systems Security. http://www.sdl.sri.com/emerald/gateway98.ps.gz.
19. U.S. Drawing Plan That Will Monitor Computer Systems. — New York Times от 28 июля 1999 года в изложении Edupage (July 28, 1999). http://listserv.educase.edu/archives/edupage.html.
20. Wood M. Inrusion Detection Exchange Format Requirements. — Internet-Draft, June 1999. http://www.ietf.org/internet-drafts/draft-ietf-idwg-requirements-00.txt.
21. Kahn C., Porras P., Staniford-Chen S., Tung B. A Common Intrusion Detection Framework. — Draft submission to a nice publication, July 1998. http://seclab.cs.ucdavis.edu/cidf/papers/jcs-draft/cidf-paper.ps.
22. Crosbie M., Price K. Intrusion Detection Systems. — Purdue University, COAST Laboratory. http://www.cs.purdue.edu/coast/intrusion-detection/ids.html.
23. Neumann P., Porras. P. Experience with EMERALD to Date. — Proceedings of the 1st USENIX Workshop on Intrusion Detection and Network Monitoring. Santa Clara, California, 11-12 April 1999. http://www.sdl.sri.com/emerald/det99.ps.gz.
24. Ranum M., Landfield K., Stolarchuk M., Sienkiewicz M., Lambeth A., Wall E. Implementing A Generalized Tool For Network Monitoring. — Proceedings of the 11th Systems Administration Conference (LISA '97), San Diego, California, October 26-31, 1997. http://www.nfr.com/forum/publications/LISA-97.htm.
25. NFR Intrusion Detection Appliance. Version 3.0. Monitor, Examine, Uncover, Empower. — Network Flight Recorder Inc., 1999. http://www.nfr.net/products/ida-facts.html.
26. Durst R., Champion T., Witten B., Miller E., Spagnulol L. Testing and Evaluating Computer Intrusion Detection Systems. — Communicaions of the ACM, July 1999/Vol. 42, No. 7, pp. 53-61. http://www.acm.org/pubs/articles/journals/cacm/1999-42-7/p53-durst/.

9. Приложение. Возможные критерии оценки систем активного аудита

Предлагаемые критерии имеют много общего с критериями оценки систем управления из статьи [6]. Это не случайно, так как активный аудит и управление по сути своей близки.

9.1. Общие положения

Под подозрительной активностью понимается поведение пользователя или компонента информационной системы, являющееся нетипичным для данного пользователя (компонента) или (в соответствии с заранее определенными критериями) злоумышленным.

Рассматриваемые в данных критериях системы должны выявлять подозрительную активность и предоставлять средства для автоматического реагирования на нетипичные или злоумышленные действия. Кроме того, они должны удовлетворять общим требованиям к сервисам информационной безопасности.

Основными показателями, характеризующими системы активного аудита, являются:

- спектр контролируемых объектов;
- спектр и степень детальности отслеживаемых характеристик;
- расширяемость системы;
- настраиваемость системы;
- степень автоматизации функционирования системы;
- возможность работы в рамках распределенных систем;
- возможность работы в реальном масштабе времени;
- технологичность системы.

9.2. Показатели, используемые для оценки систем активного аудита

Выделяются следующие показатели:

9.2.1. Отслеживание поведения пользователей и компонентов информационной системы

1) Возможность отслеживания базового набора характеристик поведения пользователей и компонентов информационной системы
2) Возможность изменения (в том числе пополнения) набора отслеживаемых характеристик
3) Возможность отслеживания характеристик в распределенных системах
4) Возможность отслеживания поведения отдельных пользователей и компонентов информационной системы в реальном масштабе времени
5) Возможность задания способа информирования администратора безопасности о выходе отслеживаемых характеристик за допустимые рамки
6) Возможность задания способа автоматического реагирования на выход отслеживаемых характеристик за допустимые рамки

9.2.2. Обеспечение конфиденциальности и целостности регистрационной информации

1) Защита регистрационной информации от несанкционированного доступа в рамках отдельных систем
2) Контроль целостности (взаимной согласованности) регистрационной информации в рамках распределенных систем
3) Защита регистрационной информации от несанкционированного доступа в рамках распределенных систем
4) Возможность задания способа информирования администратора безопасности о нарушении целостности и/или конфиденциальности регистрационной информации
5) Возможность задания способа автоматического реагирования на нарушение целостности и/или конфиденциальности регистрационной информации

9.2.3. Выявление злоумышленного поведения

1) Возможность выявления базового набора злоумышленных действий
2) Возможность пополнения базы правил, описывающих злоумышленные действия
3) Возможность настройки базы правил на конкретные информационные сервисы
4) Возможность выявления злоумышленных действий, распределенных во времени
5) Возможность выявления злоумышленных действий в распределенных системах
6) Возможность выявления злоумышленных действий в реальном масштабе времени
7) Возможность задания способа информирования администратора безопасности о выявленных злоумышленных действиях
8) Возможность задания уровня детализации информации, подтверждающей наличие злоумышленных действий
9) Возможность задания способа автоматического реагирования на выявленные злоумышленные действия

10) Наличие средств автоматической проверки согласованности базы правил в рамках распределенной конфигурации
11) Наличие средств анализа злоумышленных действий с выдачей рекомендаций по предотвращению подобных действий в будущем
12) Наличие средств прогнозирования злоумышленных действий

9.2.4. Выявление нетипичного поведения

1) Наличие подсистемы статистического анализа для выявления нетипичного поведения
2) Возможность выявления нетипичного поведения при использовании базового набора информационных сервисов
3) Возможность пополнения и/или изменения набора контролируемых аспектов поведения
4) Возможность настройки на конкретные информационные сервисы
5) Наличие средств для изменения параметров статистического анализа с целью обеспечения заданного соотношения между ошибками первого рода (отсутствие реакции на нетипичное поведение) и ошибками второго рода (ложное срабатывание)
6) Возможность выявления нетипичного поведения в рамках распределенной системы
7) Возможность выявления нетипичного поведения в реальном масштабе времени
8) Возможность задания способа информирования администратора безопасности о выявленном нетипичном поведении
9) Возможность задания уровня детализации информации, подтверждающей наличие нетипичного поведения
10) Возможность задания способа автоматического реагирования на выявленное нетипичное поведение
11) Наличие средств автоматической проверки согласованности статистических параметров в рамках распределенной конфигурации
12) Наличие средств автоматической оценки соотношения между ошибками первого и второго рода при заданных статистических параметрах

9.2.5. Администрирование

1) Идентификация и аутентификация администраторов в рамках локальных систем
2) Идентификация и аутентификация администраторов в рамках распределенных систем
3) Регистрация административных действий в рамках локальных систем
4) Регистрация административных действий в рамках распределенных систем
5) Возможность централизованного выявления подозрительной активности в рамках распределенных систем
6) Возможность централизованного администрирования распределенных систем активного аудита

9.2.6. Контроль целостности

1) Наличие средств контроля целостности программной и информационной частей системы активного аудита (локальные, распределенные, использующие аттестованные алгоритмы)

9.2.7. Масштабируемость

1) Наличие средств масштабирования по числу отслеживаемых пользователей и компонентов информационной системы: возможность группирования пользователей (компонентов) с однородными характеристиками
2) Наличие средств масштабирования по размеру обслуживаемой информационной системы, возможность варьирования между распределенной и централизованной обработкой регистрационной информации, возможность организации иерархии обрабатывающих центров

9.2.8. Доступность

1) Наличие средств обеспечения высокой доступности: сбои и отказы отдельных подсистем или компонентов системы активного аудита не должны нарушать работоспособность других подсистем (компонентов)

9.2.9. Восстановление

1) Наличие средств восстановления после сбоев и отказов, в том числе отказов отдельных элементов распределенной системы

9.2.10. Документация

1) Руководство администратора системы активного аудита (локальные, распределенные, с использованием аттестованных алгоритмов контроля целостности)
2) Руководство программиста (описание программных интерфейсов с системой сбора и анализа регистрационной информации)
3) Конструкторская (проектная) документация
4) Тестовая документация

9.2.11. Тестирование

1) Обеспечение возможности регламентного тестирования средств сбора регистрационной информации, подсистем выявления злоумышленного и нетипичного поведения,

средств контроля целостности, средств администрирования, средств восстановления

9.3. Классификация систем

Системы активного аудита разделены на пять классов (пятый — самый слабый, первый — самый сильный).

Пятый класс поддерживает базовый набор возможностей (отслеживание фиксированного набора характеристик в локальной конфигурации).

Системы четвертого класса должны обладать свойствами расширяемости и настраиваемости.

Системы третьего класса должны предоставлять базовые средства выявления нетипичной и злоумышленной активности, а также поддерживать распределенные конфигурации.

Системы второго класса должны работать в реальном масштабе времени и обладать свойством программируемости.

Системы первого класса должны обеспечивать выдачу рекомендаций по пресечению и недопущению повторных злоумышленных действий, в них должны использоваться аттестованные алгоритмы обеспечения конфиденциальности и целостности в распределенных конфигурациях.

Параллельно с требованиями к основным характеристикам ужесточаются требования к технологическим параметрам, таким как масштабируемость, восстановление и т.д.

В табл. 1 показано, как приведенные выше требования нарастают по классам. Знак «+» означает появление новых требований, знак «=» — сохранение требований предыдущего класса, знак «-» — отсутствие требований.

Показатели защищенности	Классы защищенности				
	5	4	3	2	1
1. Отслеживание поведения пользователей и компонентов информационной системы	+	+	+	=	=
2. Обеспечение конфиденциальности и целостности регистрационной информации	+	=	+	=	+
3. Выявление злоумышленного поведения	+	+	+	+	+
4. Выявление нетипичного поведения	+	+	+	+	+
5. Администрирование	+	=	+	=	=
6. Контроль целостности	+	=	+	=	+
7. Масштабируемость	-	-	+	=	+
8. Доступность	-	-	+	=	+
9. Восстановление	+	=	+	=	+
10. Документация	+	=	+	=	+
11. Тестирование	+	+	+	+	+

Табл. 1. Нарастание по классам требований к системам активного аудита.

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания Джет Инфо Паблишер

Главный редактор: Галатенко В.А. *(galat@jet.msk.su)*
Технический редактор: Антонов А.Н. *(silver@jet.msk.su)*

Россия, 103006, Москва, Краснопролетарская, 6
тел. (095) 972 11 82, 972 13 32
факс (095) 972 07 91
e-mail: JetInfo@jet.msk.su, http://www.jetinfo.com

Подписной индекс по каталогу Роспечати 32555