А. В. Аграновский (д. т. н., профессор), Р. Н. Селин
ФГНУ НИИ «Спецвузавтоматика», г. Ростов-на-Дону,
Н. Г. Милославская (к. т. н., доцент), А. И. Толстой (к. т. н., доцент)
Московский инженерно-физический институт (государственный университет)

АНАЛИЗ СОВРЕМЕННЫХ ПОДХОДОВ К ОБНАРУЖЕНИЮ КОМПЬЮТЕРНЫХ ВТОРЖЕНИЙ И ИХ НЕДОСТАТКОВ

1. Введение

Системы обнаружения сетевых вторжений (здесь и далее мы будем пользоваться определениями терминов «вторжение», «атака» и прочих в том виде, как они даны в книге [1. С. 18—20]) и выявления признаков компьютерных атак на информационные системы (ИС) уже давно применяются как один из необходимых рубежей обороны ИС. Разработчиками систем защиты информации и консультантами в этой области активно применяются такие понятия (перенесенные из направления обеспечения физической безопасности), как защита «по периметру», «стационарная» и «динамическая» защита, стали появляться собственные термины, например, «проактивные» средства защиты.

Исследования в области обнаружения вторжений в компьютерные сети и системы на самом деле ведутся за рубежом уже больше четверти века. Исследуются признаки атак, разрабатываются и эксплуатируются методы и средства обнаружения попыток несанкционированного проникновения через системы защиты, как межсетевой, так и локальной, на логическом и даже на физическом уровнях. В действительности сюда можно отнести даже исследования в области ПЭМИН, поскольку электромагнитный тампериг имеет свои прямые аналоги в уже ставшей обычной для рядового компьютерного пользователя сетевой среде. На российском рынке широко представлены коммерческие системы обнаружения вторжений (СОВ) иностранных компаний -(ISS RealSecure, NetPatrol, Snort, Cisco и т.д.) и в то же время практически не представлены комплексные решения российских разработчиков. Это вызвано тем, что многие отечественные исследователи и разработчики реализуют СОВ, сохраняя аналогии архитектур и типовых решений уже известных систем, не особенно стараясь увеличить эффективность превентивного обнаружения вторжений и реагирования на них. Конкурентные преимущества в этом сегменте российского рынка достигаются обычно за счет существенного снижения цены и упования на «поддержку отечественного производителя».

На сегодняшний день СОВ обычно представляют собой программные или аппаратно-программные решения, которые автоматизируют процесс сбора, хранения и анализа (контроля) событий, протекающих в компьютерной системе или сети, а также самостоятельно анализируют эти события в поисках признаков нарушения информационной безопасности (ИБ). Поскольку количество различных типов и способов организации несанкционированных проникновений в чужие компьютерные сети за последние несколько

лет значительно увеличилось, СОВ стали необходимым компонентом инфраструктуры безопасности большинства организаций. Этому способствует и огромное количество литературы, и стремительное появление все более изощренных и сложных подходов и методов к обнаружению вторжения в ИС.

Современные СОВ имеют различную архитектуру. На данный момент можно разделить все системы на сетевые (network-based) и системные (host-based) – это общепринятая классификация. Впрочем, классификации СОВ следует уделить отдельное внимание, поскольку зачастую, используя общепринятую классификацию СОВ, специалисты принимают решение о том, какой из программных продуктов применить в той или иной ситуации.

Сетевые системы обычно устанавливаются на выделенных для этих целей компьютерах и анализируют трафик, циркулирующий в компьютерной сети. Системные СОВ размещаются на отдельных компьютерах, нуждающихся в защите, и анализируют различные события (действия пользователя или программные вызовы).

Также различают методики обнаружения аномалий (в иностранной литературе употребляется термин-аналог «аномальное поведение») и обнаружения злоумышленного поведения (злоупотреблений) пользователей. Системы обнаружения аномалий (от англ. anomaly detection) основаны на том, что СОВ известны некоторые признаки, характеризующие правильное или допустимое поведение объекта наблюдения. Аномалией считается любое действие наблюдаемого объекта, которое не вписывается в привычный для него шаблон поведения, который может быть зафиксирован в виде экспертных правил, шаблона действий или сигнатуры. Под «нормальным» или «правильным поведением» понимаются действия, выполняемые объектом и не противоречащие политике безопасности. Системы обнаружения злоумышленного поведения (от англ. misuse detection) основаны на том, что заранее известны некоторые признаки, характеризующие поведение злоумышленника. Таким образом, системы обнаружения аномалий предназначены для поиска злоумышленных действий, которые на момент проверки не попали в экспертную базу данных, а системы обнаружения злоумышленного поведения основаны на сигнатурном или шаблонном поиске. Наиболее популярной реализацией технологии обнаружения злоумышленного поведения являются экспертные системы. Представительным западным аналогом такой системы является бесплатно распространяемая и наиболее популярная система Snort [7].

Поведенческие методы ОВ предполагают, что вторжение обнаруживается при выявлении отклонений от нормального или ожидаемого поведения системы или пользователя. Такое ОВ выполняет *поведенческая СОВ* (behavior-based IDS), *или система обнаружения аномалий* (СОА) (anomaly IDS). Для поведенческой СОВ на основе статистической информации, собранной и обработанной различными средствами, строится *профиль* — модель нормального, или допустимого, поведения (поэтому такие СОВ еще называются profile-based IDS). В полученной для анализа информации СОВ выделяет отдельные факты (зарегистрированные данные) и для выявления аномалий осуществляет сравнение наблюдаемого поведения с ожидаемыми нормальными профилями использования (т. е. «не-атаками»), которые могут быть разработаны для пользователей, групп пользователей, приложений, сетевых соединений, системных ресурсов и т.п. Принцип работы СОВ заключается в анализе того, что составляет «нормальный», типичный сетевой трафик. В этом случае работа начинается с этапа сбора данных (накопления статистики). Затем на их основе разрабатывается набор моделей поведения (профилей), которые обновляются с течением времени, — это этап обучения. Для каждого профиля вводится набор статистических метрик, описывающих типичное поведение объекта. Как СиСОВ, так и ССОВ могут реализовывать метод обнаружения аномалий в своей работе.

Интеллектуальные методы ОВ применяют знания, накопленные о специфических атаках и уязвимостях систем. *Интеллектуальные СОВ* (knowledge based IDS), или *системы обнаружения злоупотреблений* (СОЗ) (misuse IDS), содержат информацию об этих уязвимостях и ищут попытки их использования (включая запуск эксплойтов). При обнаружении такой попытки в анализируемом трафике (при этом должны контролироваться все пакеты!) поступает сигнал тревоги. При этом под

злоупотреблением часто понимаются действия, выполняемые в рамках имеющихся полномочий, но нарушающие политику ИБ. Другими словами, любое действие, которое явно не описано соответствующим формальным образом, например, в виде *сигнатуры* (от англ. signature), и, значит, не отнесено к категории атак, считается нормальным за определенный период времени.

2. Анализ недостатков современных систем обнаружения вторжений

С учетом сказанного выше все СОВ можно разделить (с точки зрения предмета анализа) на системы, ориентированные на поиск:

— аномалий взаимодействия контролируемых объектов;

— сигнатур всех узнаваемых атак;

— искажения эталонной профильной информации.

Описание «атаки», как и описание действия, не являющегося «атакой», подразумевает определение набора параметров, подлежащих наблюдению и анализу, поэтому такой набор классов позволяет разделить системы, анализирующие информацию из различных источников ее возникновения.

Необходимо отметить, что на сегодняшний день практически отсутствуют системы гибридного типа, а также системы, использующие информацию распределенного во времени и пространстве характера [9]. В ходе работы подавляющего большинства современных систем используется только сигнатурный метод распознавания атакующих воздействий или только поиск аномалий в поведении контролируемой сети.

Еще одним недостатком почти всех известных систем является отсутствие встроенного имитатора атак (работающего по принципу сканеров безопасности, или security scanners) или любого другого средства для проверки корректности развернутой и эксплуатируемой СОВ, которые обеспечивали бы возможность простого и надежного тестирования конфигурационных параметров, использованных в каждой конкретной компьютерной сети.

Данное средство по логическим соображениям должно позволять имитировать деятельность программного обеспечения вирусного типа (например, CodeRed, NetSky, Bagle, MSBlast и т.д.), атак типа «отказ в обслуживании» (например, «SYN-бомбардировка» или атака типа fraggle), атак с целью повышения привилегий учетной записи (как пример можно привести уязвимости в сетевых службах MS SQL Server 2000, MS Internet Information Service 5.0), атак с целью перенаправления трафика и навязывания ложных данных (подмена ARP и навязывание DNS-службы). При этом желательно, чтобы программное средство имело возможность генерировать атаки распределенного характера.

Например, архитектура некоторых типов имитаторов СОВ состоит из набора агентов различных типов, специализированных для решения подзадач обнаружения вторжений. Агенты размещаются на отдельных компьютерах системы. В данной архитектуре в явном виде отсутствует «центр управления» семейством агентов — в различных случаях ведущим может становиться любой из агентов, инициирующий или реализующий функции кооперации и управления. В случае необходимости агенты могут как клонироваться (осуществлять свое копирование в сетевой и локальной среде), так и прекращать свое функционирование, что очень точно передает характер большинства компьютерных вторжений. В зависимости от ситуации (вида и количества атак на компьютерные сети, наличия вычислительных ресурсов для выполнения функций защиты) может потребоваться генерация нескольких экземпляров агентов каждого класса. Предполагается, что архитектура системы может адаптироваться к реконфигурации сети, изменению трафика и новым видам атак, используя накопленный опыт.

Архитектура многоагентной системы интересна и перспективна для дальнейшего рассмотрения. Однако, к сожалению, в отечественных работах нет указаний на используемые или разработанные алгоритмы обнаружения вторжений в многоагентной системе. Кроме того, текущие версии известных имитаторов не функционируют в реальном режиме времени (поскольку этого не позволяет делать выбранный базовый инструментарий).

Вообще говоря, отсутствие имитаторов атак для оценки эффективности СОВ не является основной проблемой данного направления. Реальные недостатки существующих СОВ — примитивность простого сигнатурного поиска, малая эффективность при обнаружении распределенных по времени и месту сложных вторжений, недостаточная интеграция информации на уровне хоста и сети для обнаружения комбинированных вторжений и несанкционированных проникновений.

Среди эксплуатационных недостатков современных СОВ можно отметить большое количество вычислительных операций для простого деления принадлежности события на «свой — чужой» и невозможность обработки всей поступающей информации в реальном режиме времени на обычных персональных компьютерах. Скорость обработки сетевого или иного трафика событий зачастую медленнее реального времени в 1,5—2 раза. В некоторых системах анализ и вовсе происходит в отложенном режиме. Это означает, что реализация атаки на защищаемые информационные и вычислительные ресурсы не будет замечена вовремя (в реальном или близком к реальному времени) и уж тем более не будет отражена с помощью имеющихся средств защиты. В данном режиме СОВ может быть использована в лучшем случае как средство журналирования всех этапов атаки и последующей криминалистической экспертизы.

При этом большинство современных СОВ изначально не разрабатываются «портируемыми», то есть их код не переносится на различные операционные системы и произвольные аппаратно вычислительные платформы. Работа на нескольких операционных системах для большинства западных продуктов и почти всех отечественных СОВ (как экспериментальных, так и коммерчески адаптированных) невозможна. С учетом того, что СОВ не используют преимущества разработки и оптимизации кода для выбранных операционных систем и аппаратных платформ, это их один из самых существенных недостатков.

Кроме того, ни в одной программной или аппаратно-программной системе не предусмотрен режим «горячего резерва», позволяющий в случае выведения из строя основного комплекса оперативно ввести в работу комплекс «горячего резервирования» и тем самым восстановить уничтоженный рубеж обороны сетевого периметра. Несмотря на это, есть и положительный момент в развитии СОВ, который заключается в стремлении разработчиков интегрировать свои системы с существующими средствами защиты (межсетевыми экранами, сканерами защищенности, блокираторами каналов, QoS диспетчерами).

2.1. Анализ систем, использующих сигнатурные методы

Сигнатурные методы позволяют описать атаку набором правил или с помощью формальной модели, в качестве которой может применяться символьная строка, семантическое выражение на специальном языке и т.п. Суть данного метода заключается в использовании специализированной базы данных шаблонов (сигнатур) атак для поиска действий, подпадающих под определение «атака».

Сигнатурный метод может защитить от вирусной или хакерской атаки, когда уже известна сигнатура атаки (например, неизменный фрагмент тела вируса) и внесена в базу данных СОВ, то есть, когда сеть переживает первое нападение извне, первое заражение еще неизвестным вирусов и в базе попросту отсутствует сигнатура для его поиска, сигнатурная СОВ не сможет сигнализировать об опасности, поскольку сочтет атакующую деятельность легитимной.

Кроме того, несмотря на кажущуюся простоту сигнатурного метода и в его реализации есть свои тонкости. Классический пример: с помощью поиска сигнатуры

/../../../../../../../../local.ida

и простого сравнения битовой информации невозможно выявить хакерскую атаку на HTTP-сервер. Нападающий может легко изменить строку в соответствии с соглашением об URI и использовать битовую строку

%2F%2E%2F%2E%2F%2E%2F%2E%2F%2E%2F%2E%2F%2Elocal.ida,

которую данная сигнатура уже не охватывает [7].

Большинство существующих программных продуктов, заявляющих об использовании сигнатурного метода, на самом деле реализуют как раз наиболее примитивный способ сигнатурного распознавания. К ним относятся и западные, и практически все отечественные разработки. Многие системы позиционируются как предназначенные для выявления атак в ИС на основе интеллектуального анализа сетевых пакетов. На самом же деле сигнатурный метод реализован как алгоритм, исследующий лишь динамику развития атаки, основанный на автомате состояний для оценки сценария развития атаки. По замыслу такой подход должен позволить отследить динамику развития атаки в соответствии с действиями злоумышленника, при этом в качестве модуля сбора данных могут использоваться даже сами системы обнаружения вторжений.

Однако на практике, например, применение для сбора данных системы Snort сильно замедляет процесс обнаружения, что не позволяет осуществлять анализ в реальном режиме времени (хотя оригинальная СОВ Snort работает в режиме, близком к реальному времени). С другой стороны, такая система становится очень сложна из-за использования большого количества конфигурационных параметров и переусложнения схемы обработки данных.

Таким образом, эффективность работы сигнатурной СОВ определяется тремя основными факторами:

· оперативностью пополнения сигнатурной базы;

· ее полнотой с точки зрения определения сигнатур атак;

· наличием интеллектуальных алгоритмов сведения действий атакующих к некоторым базовым шагам, в рамках которых происходит сравнение с сигнатурами.

Для успешной реализации первых двух факторов необходима поддержка международных стандартов и рекомендаций (например, Intrusion Detection Message Exchange Requirements) по обмену сигнатурами и информацией об атаках. Поскольку на данный момент не существует достаточно большого количества распределенных и объективных источников сигнатур, то СОВ данного типа имеют весьма лимитированную эффективность в реальных сетях.

2.2. Анализ систем, использующих методы поиска аномалий в поведении

Системы поиска аномалий идентифицируют необычное поведение («аномалии») в функционировании контролируемого объекта. В качестве объекта наблюдения может выступать сеть в целом, отдельный компьютер, сетевая служба (например, файловый сервер FTP), пользователь и т.д. Сигнализация СОВ срабатывает при условии, что действия, совершаемые при нападении, отличаются от «обычной» (то есть законной, санкционированной) деятельности пользователей и компьютеров. Меры и методы, обычно используемые при обнаружении аномалии, включают использование:

— пороговых значений (наблюдения за объектом выражаются в виде числовых интервалов);

— статистических мер (решение о наличии атаки делается по большому количеству собранных данных);

— профилей (для выявления атак на основе заданной политики безопасности строится специальный список легитимных действий — «профиль нормальной системы»);

— нейронных сетей, генетических алгоритмов.

Отличительной чертой данных систем является необходимость их обучения «стандартному» поведению контролируемого объекта (например, корпоративной интрасети). Это же является и основным недостатком всех подобных методов, поскольку время обучения составляет довольно большой промежуток времени, и все это время на контролируемые объекты не должно быть произведено ни единой атаки. В случае если защищаемая интрасеть на этапе обучения отключается от других сетей, то на этапе эксплуатации система защиты будет классифицировать все попытки легального взаимодействия с внешними сетями как атаки.

В случае создания СОВ, использующей профильные системы, следует учитывать, что по разным исследованиям, как минимум, 15% пользователей компьютерных сетей не подлежит профилированию вообще, а еще столько же имеет тенденцию к быстрому изменению поведения в течение ограниченного времени. Статичность существующих профильных систем позволяет говорить об этом как об одном из основных недостатков, явно мешающих эксплуатации СОВ на базе контроля «профилей» пользователей.

В случае динамической подстройки и модификации профилей необходимо найти компромисс между количеством признаков профилирования (чем их меньше, тем грубее оценивается поведение контролируемого объекта) и скоростью обработки (скорость оценки аномальности поведения по профилю является экспоненциальной функцией от количества исследуемых признаков). Кроме того, большое число конфигурационных параметров в этом случае неизбежно потребует от администратора системы защиты высокой квалификации в весьма специализированной области обнаружения вторжений.

Такой подход реализован в некоторых отечественных СОВ. Данные разработки относятся к классу системных СОВ, их экземпляры должны эксплуатироваться на каждом информационном ресурсе, нуждающемся в защите. Особенностью одной из данных систем является использование процедур нечеткого поиска. Для каждого пользователя создается свой индивидуальных профиль, при этом поведение, характерное для одного из пользователей, может считаться необычным для другого, и наоборот. Поскольку такие профили трудно формализовать, они создаются на основе примеров нормальной работы того или иного пользователя. В качестве показателей активности пользователей выбраны запуск и завершение приложений, а также переход от одного активного приложения к другому. Профили создаются на основе примеров нормальной работы того или иного пользователя. Для представления профилей разработчиками были выбраны нейронные сети. По данным разработчиков тестирование системы показало, что вероятность ошибки первого рода составляет 5—15%, ошибки второго рода — 10—20%. При этом до половины тестовой выборки составляли вектора пользователей, которые не участвовали в построении обучающей выборки, что говорит о хорошей обучающей способности нейронной сети.

3. Заключение

Большинство рассмотренных недостатков современных СОВ являются недостатками, с которыми может столкнуться пользователь в реальных компьютерных сетях. Большая часть замечаний о недостатках и степени эффективности разрабатываемых методов и средств происходит из практики использования СОВ в реальных корпоративных интрасетях.

Существующие подходы к решению задач обнаружения вторжений зачастую отличаются не только реализацией методов обнаружения, но и своей архитектурой, уровнем детализации и типами обнаружения вторжений. Естественно, что у каждой системы есть свои достоинства и недостатки. При этом, несмотря на постоянное развитие применяемых при разработке СОВ технологий, о легкости развертывания, эксплуатации и модификации СОВ придется забыть: все существующие разработки имеют тенденцию лишь к усложнению. Технологии взлома постоянно совершенствуются, атаки становятся комбинированными и распространяются с очень большой скоростью. И поэтому к современным СОВ предъявляются все более жесткие и сильные требования. Очевидно, что для соответствия своей задаче СОВ должны реализовывать две основные рассмотренные выше технологии, в той или иной степени взаимодополняющие друг друга.

Кроме того, немаловажными являются и аспект безопасности функционирования самих СОВ, а также их отказоустойчивость. На сегодняшний опубликовано немало примеров выведения популярных СОВ из строя путем простой посылки определенных пакетов (самый известный пример — сетевые пакеты «нулевой» длины, выводившие из строя некоторые версии СОВ Snort и даже tcpdump).

Если рассматривать СОВ с точки зрения методов обнаружения вторжений, то, очевидно, это должны быть системы, включающие в себя множество модулей, реализующих различные подходы с учетом различных типовых сегментов защищаемых сетей. Перед большинством СОВ уже стоит проблема повышения быстродействия, так как современные компьютерные сети становятся все более быстрыми. По мере внедрения СОВ в эксплуатацию повышаются требования к масштабируемости и простоте управления этими системами. В будущем СОВ видимо разделятся на две категории, которые будут использовать различные подходы для малых корпоративных сетей и для больших, сложных по своей топологии компьютерных интрасетей территориально распределенных корпораций.

Таким образом, особенности современных компьютерных сетей и требования к ним, такие как повышение надежности сетей, повышение мобильности, иерархическая структура сетей, различные требования к безопасности, накладывают отпечаток на технологии и подходы, которые должны быть уже на сегодняшний день реализованы в СОВ.

СПИСОК ЛИТЕРАТУРЫ

1. *Милославская Н. Г., Толстой А. И.* Интрасети: обнаружение вторжений. Учебное пособие для вузов. М.: ЮНИТИ-ДАНА, 2001.
2. *Лукацкий А. В.* Обнаружение атак. СПб.: БХВ-Петербург, 2001.
3. *Климовский А. А.* К анализу подходов классификации компьютерных атак // Материалы международной научной конференции по проблемам безопасности и противодействия терроризму. М.: МЦНМО, 2006.
4. *Сердюк В. А.* Анализ современных тенденций построения моделей информационных атак // Информационные технологии. 2004. № 4.
5. *Новиков А. А., Устинов Г. Р.* Уязвимость и информационная безопасность телекоммуникационных технологий. М: Радио и связь, 2003.
6. *Huang M., Wicks T. M.* A Large-scale Distributed Intrusion Detection Framework Based on Attack Strategy Analysis // Proceedings of First International Workshop on the Recent Advances in Intrusion Detection, September 14–16, 1998, Louvain-la-Neuve, Belgium.
7. *Чирилло Дж.* Обнаружение хакерских атак. СПб.: Питер, 2002.
8. *Eiter M. V.* Comparing environments for developing agents. Technical report, Technische Universitat Wien, March 2001.
9. *Аграновский А. В., Хади Р. А., Балакин А. В.* Обучаемые системы обнаружения и защиты от вторжений // Искусственный интеллект. Донецк, Украина, 2001. № 3. С. 440–444.
10. *Bace R., Mell P.* Intrusion Detection Systems // NIST Special Publication on Intrusion Detection Systems. 2001.
11. *Teresa L. F.* A Survey of Intrusion Detection Techniques // Computers and Security 12, 4 (June 1993): 405–418.
12. *Kotenko I., Man'kov E.* Agent-Based Modeling and Simulation of Computer Network Attacks // Proceedings of Fourth International Workshop Agent-Based Simulation 4 (ABS 4), Montpellier, France, 2003. P. 121–126.
13. *Kotenko I.* Teamwork of Hackers-Agents: Modeling and Simulation of Coordinated Distributed Attacks on Computer Networks // Proceedings of the 3rd International Central and Eastern European Conference on Multi-Agent Systems (CEEMAS 2003). Prague, Czech Republic, 2003. Lecture Notes in Artificial Intelligence, Springer-Verlag. Vol. 2691. P. 464–474.
14. *Медведовский И. Д., Семьянов П. В., Платонов В. В.* Атака через Internet. М., 1997.
15. *Медведовский И. Д., Семьянов П. В., Леонов Д. Г.* Атака на Internet. М.: ДМК, 1999.
16. *Медведовский И. Д., Семьянов Б. В., Леонов Д. Г., Лукацкий А. В.* Атака из Internet. М.: Солон-Р, 2002.