Мониторинг угроз компьютерного нападения на информационно-телекоммуникационные системы

В.В. Корнеев (Россия)

Место динамического мониторинга в программно-аппаратной платформе

Обеспечение информационной безопасности служит одной из составных частей управления системой, и для пользователя не важно получил он отказ в обслуживании или искажение данных в результате реализации угрозы компьютерного нападения, отказа оборудования или ошибки в программе. Опять же, после обнаружения атаки необходимо принять меры для предотвращения продолжения атаки и восстановления работоспособного состояния, что требует управления системой.

В рамках концепции открытых систем имеется и быстро развивается несколько интегрированных систем управления, таких как HP OpenView, Solstice SunNet Manager, Unicenter TNG, базирующихся на модели управления, предложенной Международной Организацией по Стандартизации (ISO). Согласно этой модели система управления призвана решать задачи 5 типов (каждый тип содержит множество различных подзадач):

1. Управление эффективностью (сбор и анализ информации об эффективности использования ресурсов по параметрам, задаваемым администратором; цель – выявление причин недостаточной производительности и др.).
2. Управление конфигурацией (сбор и анализ информации о состоянии аппаратных и программных элементов системы, управление работой различных конфигураций аппаратных средств и разных версий программного обеспечения; цель – обеспечение совместимости и нейтрализация эксплуатационных отклонений и погрешностей для поддержания надежной работы).
3. Управление использованием ресурсов (измерение параметров использования системы индивидуальными и групповыми пользователями и выделение ресурсов для них; цель – рациональное предоставление ресурсов, как с точки зрения системы, так и с точки зрения пользователя).
4. Управление неисправностями (определение симптомов неисправности, фиксация, изоляция неисправности путем реконфигурации системы, уведомление пользователей, и автоматическое устранение проблем в системе (в пределах возможного), возникающих вследствие сбоев и отказов, устранение неисправности, проверка устранения неисправности во всех важных подсистемах; цель – обеспечение отказоустойчивости и непрерывности обслуживания).
5. Управление защитой данных (контроль доступа к ресурсам в соответствии с политикой безопасности; цель – реализация политики безопасности).

Интегрированные системы управления, а также операционные системы семейства Unix, трансляторы и другое общесистемное программное обеспечение имеют ставший по существу стандартом уровень функциональности и интерфейсов прикладного программирования, который воспринимается пользователями как комфортный. Создание эквивалентной по функциональности и интерфейсам среды прикладного программирования из продуктов отечественной разработки для отечественных пользователей представляется не реальным. Поэтому необходимо создавать продукты для обеспечения информационной безопасности в рамках концепции открытых систем. Эти продукты должны осуществлять интеллектуальный контроль за программно-аппаратными платформами, на которых функционируют прикладные информационно-телекоммуникационные системы.

Место динамического мониторинга в реализации политики безопасности

Система динамического мониторинга дополняет такие традиционные защитные механизмы, как идентификация/аутентификация и разграничение доступа.

Подобное дополнение необходимо по следующим причинам:

- во-первых, существующие средства разграничения доступа не способны реализовать все требования политики безопасности, если последние имеют более сложный вид, чем разрешение/запрет атомарных операций с ресурсами информационной системы. Развитая

политика безопасности может, например, накладывать ограничения на суммарный объем прочитанной пользователем информации, запрещать доступ к ресурсу В, если ранее имел место доступ к ресурсу А, и т.п.;

- во-вторых, в самих защитных механизмах сети могут быть ошибки и уязвимости, поэтому помимо внедрения, пусть даже самых эффективных защитных механизмов, приходится заботиться и об обнаружении фактов преодоления внедренных в систему средств защиты;

- в третьих, в процессе эксплуатации защитных механизмов пользователи могут допускать нарушения правил их эксплуатации, приводящие к возможности нарушения политики безопасности.

Классификация систем динамического мониторинга

Системы динамического мониторинга могут быть классифицированы по известным в литературе признакам:

По методу обнаружения. Если для обнаружения атаки система динамического мониторинга использует информацию о ранее известных атаках, то она относится к системам, ***основанным на знаниях***. Если для обнаружения атаки система динамического мониторинга использует информацию о нормальном поведении системы, в которой осуществляется мониторинг, то система динамического мониторинга относится к системам, ***основанным на поведении***.

По поведению при обнаружении атаки. Если система динамического мониторинга активно реагирует на атаку, исправляя последствия атаки, либо прекращая обслуживание, то система называется ***активной***. Если система динамического мониторинга только генерирует сигнал тревоги, то она относится ***к пассивным***.

По источнику данных для аудита. Система динамического мониторинга относится к ***хостовым***, если использует данные из log файлов, или ***сетевым***, если анализирует пакеты, или комбинированным – при использовании log файлов и пакетов.

По типу функционирования. Системы динамического мониторинга ***непрерывного действия***, работающие в реальном времени, или ***периодически активизируемые***.

По методу принятия решения. Методы решения задач распознавания атак могут быть классифицированы на ***лингвистические*** (синтаксические, структурные) и ***геометрические***. Под атакой понимается некоторое подмножество состояний объектов системы. В качестве объектов выступают, например, поля записей в базах данных, поля в принятых пакетах, векторы прерываний и так далее. При этом из пакетов может выделяться содержимое разных сетевых уровней, производиться дефрагментация пакетов для получения возможности анализа их полного содержимого и реконструкции потоков пакетов для получения возможности учета информации о развитии атаки. Принятие решения о том, какие состояния считать атакой, относится к задачам управления и предполагает определение множества признаков объектов, установление шкал и измерение у объектов значений этих признаков, построение решающих правил распознавания классов состояний объектов по векторам признаков, представляющим эти состояния.

Лингвистические методы используют в качестве признаков некоторые заранее определенные непроизводные (исходные) элементы. Состояния объектов представляются посредством иерархической структуры, конструируемой на базе непроизводных элементов. Грамматика задания состояний содержит конечное число непроизводных элементов, правил подстановки и переменных. В лингвистических методах используется весь арсенал формальных языков и грамматик. Лингвистические методы применяются, например, при ***сигнатурном анализе***.

В **геометрических методах** состояния объектов представляются точками в многомерном пространстве признаков, число измерений которого равно числу признаков, различаемых у объектов. Ярким представителем этих методов служат ***пороговые решающие правила***, относящие к разным классам состояния, в которых значение некоторого признака больше-равно или меньше заданного порога. Геометрические методы, в свою очередь, могут быть классифицированы:

по априорной информации (полностью определенные, параметрические или непараметрические);

по используемым моделям (детерминированные или вероятностные).

Например, в этой классификации нейронные сети относятся к параметрическим детерминированным методам, в которых, в отличие от полностью определенных, не заданы

разделяющие гиперплоскости и эталоны классов, а количество и положение гиперплоскостей и эталонов классов формируется на базе обучающих примеров, путем определения соответствующих значений весовых коэффициентов, выступающих в роли параметров.

Системы динамического мониторинга должны удовлетворять следующим требованиям:

- Полнота обнаружения атак. Пропуск даже одного сетевого пакета может дать злоумышленнику шанс на успешную атаку.
- Высокая производительность и масштабируемость. Если известно, что система динамического мониторинга обладает недостаточной производительностью, она может стать объектом атаки на доступность, на фоне которой будут развиваться другие виды нападения. Это требует от системы динамического мониторинга 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.
- 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 динамического мониторинга имеет право принять "своего" за "чужого", то есть вероятность ложной тревоги должна иметь порядок не более 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 динамического мониторинга должны управляться (устанавливаться, конфигурироваться, контролироваться) наравне с другими сервисами. Во-вторых, динамический мониторинг может (и должен) поставлять данные в общую базу данных управления. Интеграция с сервисами безопасности необходима как для лучшего анализа ситуации (например, с привлечением средств контроля целостности), так и для оперативного реагирования на нарушения (средствами приложений, операционных систем или межсетевых экранов).
- Наличие технической возможности удаленного мониторинга информационной системы. Такая возможность, несмотря на ее потенциальную уязвимость, вполне оправдана, поскольку большинство организаций не располагает квалифицированными специалистами по информационной безопасности во всех пунктах распределенной информационно-телекоммуникационной системы.

Стандарты в области динамического мониторинга

1. Унификация форматов данных и протоколов обмена данными

Для развития работ в области обнаружения атак DARPA создало рабочую группу CIDF (Common Intrusion-Detection Framework). Цель этой группы – координация проектов с целью унификации форматов данных и протоколов обмена данными между средствами, разрабатываемыми в разных проектах. Выделены группы модулей в соответствии с их ролью в системах обнаружения атак (COA). Определены интерфейсы между модулями. CIDF вырабатывает Internet Engineering Task Force (IETF) с целью сделать свою работы стандартом для сети Internet.

CIDF выделяет 4 группы модулей. Модули взаимодействуют посредством объектов gidos (generalized intrusion-detection object), представленных в стандартизованном формате s-expression. Gidos переносят информацию между модулями. С семантической точки зрения, gidos представляют либо событие аудита, которое произошло в системе, либо результат анализа события аудита.

Четыре типа модулей следующие:

Событийные модули (Event boxes, сокращенно E-boxes) вырабатывают события, которые обрабатываются COA. E-boxes протекают на системе, находящейся под наблюдением, и делают доступными происходящие в системе события всем модулям COA. Роль E-boxes состоит в выдаче информации о событиях в стандартизованной форме gidos.

Анализирующие модули (Analysis boxes, сокращенно A-boxes) обрабатывают события от E-boxes и/или других A-boxes и выдают сигнал об атаке. Важно подчеркнуть, что возможно построение иерархической схемы принятия решения об атаке, например, на основании заключения нескольких A-boxes и наличия определенных событий.

Базы данных (Database boxes, сокращенно D-boxes) содержат архив gidos. Например, в D-box можно запомнить события и сигналы об атаках. Каждый модуль D-box может работать только с определенным модулем A-box, который он поддерживает.

Реагирующие модули (Response boxes, сокращенно R-boxes) вырабатывают защитные действия в соответствии с поступившим сигналом об атаке. Многие современные атаки длятся секунды или даже доли секунды, поэтому включение в процесс реагирования человека часто вносит недопустимо большую задержку. Ответные меры должны быть в максимально возможной степени автоматизированы, иначе формирование адекватного ответа во многом теряет смысл. Автоматизация нужна еще и по той причине, что далеко не во всех организациях администраторы безопасности обладают достаточной квалификацией для адекватного реагирования на идентифицированные атакующие информационные воздействия.

2. Проект стандарта ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»

Этот стандарт предусматривает класс функциональных требований FAU: аудит безопасности.

Аудит безопасности включает распознавание, запись, хранение и анализ информации, связанной с действиями, относящимися к безопасности (например, действиями, контролируемыми политикой безопасности объекта оценки).

Аудит безопасности декомпозируется на следующие компоненты:

- Автоматическая реакция аудита безопасности
- Генерация данных аудита безопасности
- Анализ аудита безопасности
- Просмотр аудита безопасности
- Выбор событий аудита безопасности
- Хранение событий аудита безопасности

Построение систем динамического мониторинга

Возможность создания систем динамического мониторинга открывается в рамках мультиагентных систем. Агенты - это программные модули, накапливающие информацию об устройстве, в котором они установлены. Агенты хранят эту информацию в специальной базе данных и, по мере необходимости, передают ее управляющим объектам с помощью протокола управления. Эти базы данных содержат сведения и управляющую информацию для каждого устройства системы. Агенты берут информацию из этих баз, совершают на основе этой информации предписанные действия и, возможно, записывают результаты своих действий в те же базы. В роли таких баз могут выступать, например, База Данных Управляющей Информации (MIB - Management Information Base) в случае использования протокола SNMP (Simple Network Management Protocol). Группа DMTF (Distributed Management Task Force) разработала общую информационную модель CIM (Common Information Model), позволяющую отображать форматы CMIP (Common Management Information Protocol), COM (Component Object Model), CORBA (Common Object Request Broker Architecture), SMNP и другие в произвольный фирменный формат данных, что позволяет интегрировать базы данных разных форматов в одной системе управления.

В настоящее время получены результаты [1, 2], позволяющие сделать заключение о возможности создания нейросетевой системы, которая может, как самостоятельно выявлять атаки на информационно-телекоммуникационные системы, так и служить средством контроля функционирования коммерческих интегрированных систем управления.

Литература

1. Корнеев В.В., Масалович А.И., Савельева Е.В., Шашаев А.Е. Распознавание программных модулей и обнаружение несанкционированных действий с применением аппарата нейросетей. Информационные технологии. № 10, 1997

2. Корнеев В.В., Сажин С.В. Система контроля за функционированием компьютеров и компьютерных сетей на основе применения нейронных сетей. Нейрокомпьютеры: разработка и применение, № 1, 2000