Алферов И. Л.
Московский инженерно-физический институт (государственный университет)

ПРЕДОТВРАЩЕНИЕ ВТОРЖЕНИЙ НА УРОВНЕ ОБЪЕКТНО-ОРИЕНТИРОВАННЫХ УСТРОЙСТВ ХРАНЕНИЯ ДАННЫХ

В статье исследуются вопросы обнаружения и предотвращения вторжений на уровне устройств хранения данных, поддерживающих объектно-ориентированные интерфейсы доступа, даются обоснования эффективности этого рубежа в комплексной системе защиты информации современной организации и предлагается подход к построению соответствующих систем предотвращения вторжений.

Эволюция гибридных и многовекторных атак, направленных на преодоление инфраструктуры безопасности информационных систем, стала причиной высоких рисков и связанных с ними финансовых потерь для организаций, что обусловило экономическую целесообразность внедрения и сопровождения систем комплексной проактивной защиты информационных активов. Важными компонентами таких систем традиционно являлись системы обнаружения вторжения (СОВ), однако в последнее время им на смену пришли системы предотвращения вторжений (СПВ) [1], обладающие в отличие от пассивного режима первых средствами активной динамической реакции на изменяющиеся угрозы. При этом большинство применяемых систем по способу сбора информации относятся либо к категории сетевых СПВ [2], либо к категории хостовых СПВ [3]. Сетевые СПВ осуществляют анализ проходящего сетевого трафика и при обнаружении атаки могут предпринимать активные ответные действия от блокировки трафика вплоть до опроса и контратаки источника. Хостовые СПВ, как правило, интегрируют в себе контроль системных вызовов, локальный межсетевой экран и антивирусную защиту, также выполняя при обнаружении атак различные ответные действия, например, интерактивный запрос на разрешение проведения операции или перенос вредоносного кода в карантин.

Можно показать, что еще одной точкой эффективного обнаружения и предотвращения вторжений является интерфейс устройства хранения данных (УХД) [4]. Если архитектура сети построена таким образом, что все постоянно хранимые данные размещаются на УХД, то через этот интерфейс проходят любые изменения в этих данных. Подавляющее большинство вторжений предполагают внесение изменений в данные в целях эскалации полномочий и сохранения состояния между перезагрузками системы, что позволяет обнаружить признаки их активности на уровне УХД.

Основная проблема, возникающая при построении СПВ уровня УХД в традиционных сетях хранения данных (СХД, англ. Storage Area Network), заключается в необходимости преобразования правил обнаружения файлового уровня к правилам блочного уровня, которым оперируют интерфейсы традиционных УХД. Фактически алгоритм обнаружения вторжений должен извлекать из блочной информации метаданные файловой системы подобно тому, как сетевые СОВ/СПВ извлекают из пакетов данные уровня приложения для дальнейшего анализа. Избежать решения этой ресурсоемкой задачи позволяет пришедшая на смену традиционным подходам технология объектного хранения данных [5], которая предполагает хранение данных и метаданных в виде объектов, независимо от того, представляют ли они собой файлы, записи базы данных или сущности какой-то иной природы.

В стандартной модели безопасности для объектно-ориентированных СХД предусмотрено использование классической мандатной схемы для разграничения доступа клиентов сети к информационным объектам. Этот механизм предотвращает большинство несанкционированных действий, однако не позволяет обнаруживать и противодействовать успешным вторжениям в систему, когда нарушитель становится обладателем реквизитов и прав доступа легитимных клиентов сети. Поэтому задача предотвращения вторжений на уровне объектно-ориентированных УХД (англ. Object Storage Device, OSD) является комплементарной к задаче разграничения доступа и не менее актуальна, чем для традиционных УХД.

В статье исследуются вопросы создания СПВ уровня объектно-ориентированных УХД, а также обосновывается эффективность их применения в качестве базовых механизмов защиты информационных систем.

1. Обнаружение вторжений на уровне объектно-ориентированных УХД

На рис. 1 продемонстрировано использование различных типов систем предотвращения вторжений в рамках простой информационной системы. Каждая из них решает собственный класс задач:

· сетевая СПВ — обнаружение и предотвращение атак, связанных с передачей трафика через контролируемый СПВ сегмент сети;

· хостовая СПВ — обнаружение и предотвращение атак на контролируемый узел сети, в том числе сетевых, вирусных и прочих, связанных с превышением полномочий;

· СПВ уровня УХД — обнаружение и предотвращение атак, связанных с доступом к информации, хранимой на УХД.

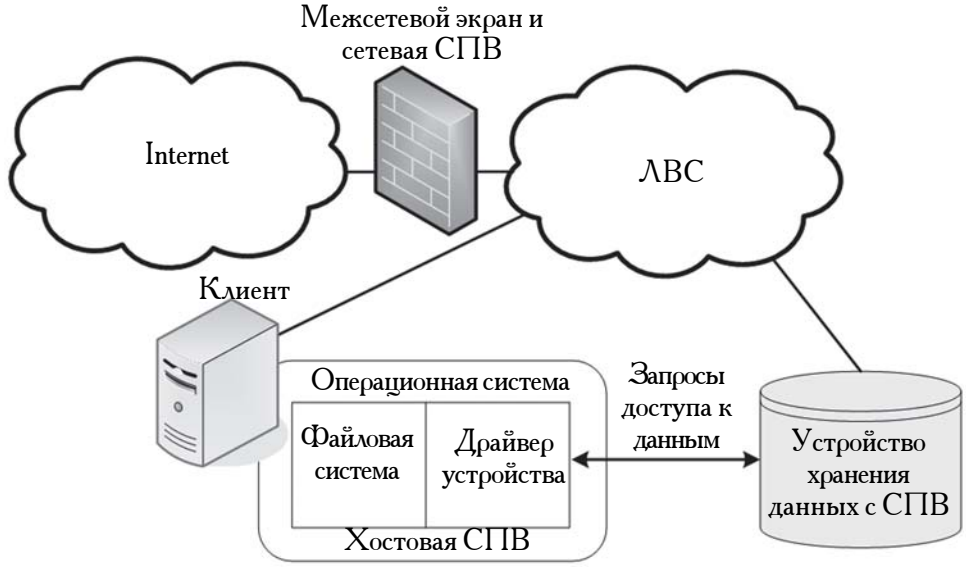

Рис. 1. Типы систем предотвращения вторжений

Перечисленные типы СПВ дополняют друг друга, но не заменяют. Тем не менее, исследования [6] показывают, что обнаружение вторжений на уровне УХД позволяет выявить подавляющее большинство атак на узлы сети, так как они тем или иным образом обращаются к хранимым данным, например, изменяя бинарные данные, модифицируя протоколы аудита или используя подозрительные имена файлов. Это позволяет в случае совместного использования УХД узлами сети применять их как адекватную альтернативу повсеместной установке хостовых СПВ, значительно сокращая тем самым издержки, связанные с обеспечением безопасности. Действительно, хостовые СПВ требуют массового тиражирования и сопровождения, а значительное использование ими системных ресурсов ведет к общему снижению производительности контролируемых узлов. Поэтому использование хостовых СПВ представляется целесообразным только для критических узлов сети, таких как серверы онлайн-сервисов или серверы корпоративного документооборота. Кроме того, СПВ уровня УХД обладают возможностью противостоять атакам и сохранять целостность данных даже в случае компрометации узлов сети и обхода хостовых СПВ. Компрометация же СПВ уровня УХД сильно затруднена тем, что УХД предоставляют фиксированные ограниченные интерфейсы доступа к ним, такие набор команд SCSI, и вероятность нахождения бреши в этих интерфейсах мала.

Еще одной особенностью СПВ уровня УХД является возможность препятствовать распространению атаки внутри сети. Например, вредоносный код в целях своего распространения часто инфицирует файлы и приложения, размещенные в разделах совместного доступа пользователей.

Однажды проникнув на совместно используемое УХД, вирус может оставаться там длительное время, заражая все новые и новые узлы сети и потенциально инициируя эпидемию с дорогостоящими для организации последствиями. СПВ уровня УХД могут включать в себя функции антивирусной защиты и эвристического анализа, позволяющие предотвратить сохранение вредоносного кода и тем самым свести к минимуму возможность его распространения через системы хранения данных.

В зависимости от топологии сети, способов ее использования и применяемого набора средств защиты информации та или иная конфигурация размещения различных типов СПВ может быть более или менее эффективной. Ответ на вопрос выбора конфигурации может дать проведение полного анализа и управления рисками в информационной системе [7], однако, исходя из вышесказанного, можно отметить следующие основания для использования СПВ уровня УХД:

- высокий уровень надежности (сложность компрометации);
- эффективное обнаружение атак, обращающихся к хранимой на УХД информации;
- возможность обнаружения вторжений в случае компрометации других устройств сети;
- повышение общей вероятности обнаружения вторжений в систему;
- возможность оперативного реагирования и предотвращения распространения вторжений;
- ведение аудита и повышение информационного сопровождения для проведения расследований инцидентов нарушения безопасности.

Традиционная архитектура систем хранения данных предполагает блочные интерфейсы взаимодействия между клиентами и УХД, когда отображением структуры файловой системы на подмножества блоков занимается драйвер этой файловой системы, установленный на клиентской стороне. Так как процессы прикладного уровня при этом обычно оперируют не блоками данных, а файлами, правила обнаружения вторжений также всегда строятся в терминах файловых операций. Как уже отмечалось, это порождает проблему преобразования правил файлового уровня в правила блочного уровня так, чтобы входящие запросы к УХД могли быть проверены СПВ на наличие признаков вторжения. В исследованиях для решения этой проблемы было предложено несколько усложненных концепций, таких, например, как семантические интеллектуальные дисковые системы (СИДС, англ. Semantically-Smart Disk System) [8], обладающие детальными знаниями о поведении находящихся выше файловых систем и используемых ими структурах размещения данных.

Нужда в сложной логике преобразования правил отпадает при использовании технологии объектного хранения данных, в которой доступ к УХД осуществляется по объектно-ориентированному интерфейсу. Большая часть функций, выполняемых драйвером файловой системы, таких как управление дисковым пространством, кэширование, синхронизация и разграничение доступа, переносится при этом в набор штатных функций объектно-ориентированного УХД. Обладая высокими вычислительными мощностями, информацией о специфике хранимых объектов и непосредственным низкоуровневым доступом к физическим носителям информации, объектно-ориентированное устройство позволяет значительно повысить как производительность операций работы с данными, так и их безопасность. Помимо этого, объектно-ориентированные УХД обладают развитыми интерфейсами взаимодействия с другими узлами сети, что позволяет использовать их для оперативного распространения сигналов тревоги при обнаружении вторжений.

Построение СПВ на уровне объектно-ориентированных УХД позволяет использовать весь расширенный функционал, имеющийся в их совместном распоряжении. Например, СПВ может требовать инкрементального сохранения версий всех изменяемых объектов в течение некоторого промежутка времени, называемого окном обнаружения, чтобы иметь возможность восстановить данные в случае обнаружения вторжения на поздних этапах. Такой подход был исследован для традиционных систем хранения данных [9] и признан достаточно эффективным.

Таким образом, предотвращение вторжений на уровне объектно-ориентированных УХД по сравнению с традиционным подходом обладает дополнительными преимуществами.

· Отсутствие потребности в преобразовании правил обнаружения вторжений файлового уровня в правила блочного уровня.

· Повышенная вычислительная мощность объектно-ориентированных УХД позволяет использовать сложные цепочки правил и гибридные схемы обнаружения вторжений без существенного влияния на производительность выполнения основных операций.

· Коммуникационные интерфейсы объектно-ориентированных УХД позволяют обеспечить немедленное оповещение о подозрительной активности.

· Возможность использования функций предотвращения вторжений в сочетании с версионностью объектов для минимизации последствий атак на систему.

2. Модель нарушителя и принципы предотвращения вторжений

Так как доступ к системам хранения данных осуществляется опосредованно, для того, чтобы его получить нарушитель должен либо являться внутренним, либо успешно скомпрометировать один или более узлов сети. Поэтому СПВ уровня УХД должны ориентироваться главным образом на обнаружение признаков активности нарушителей, уже обладающих контролем над некоторыми узлами сети и располагающими реквизитами доступа легитимных клиентов. Под контролем над узлом сети подразумевается возможность запуска на нем произвольного программного обеспечения с привилегиями уровня операционной системы. Компрометация узла может быть достигнута как техническими (использование ошибок в программном обеспечении, пробелов в политике безопасности), так и нетехническими (социальная инженерия, взяточничество) методами.

Обнаружение нарушителей, обладающих частичным контролем над сетью и использующим различные методы скрытия своего присутствия, представляет собой сложную задачу для классических хостовых и сетевых СПВ. Существует множество программных инструментов, позволяющих при получении достаточного уровня привилегий нейтрализовать хостовые СПВ, отключая или дезинформируя их. Сетевые СПВ при этом могут продолжать мониторинг подозрительной активности, однако действия проникшего в систему нарушителя, скрывающего свое присутствие, подвержены сетевому обнаружению в значительно меньшей степени, чем его действия во время первоначальной атаки на систему [10]. В связи с этим именно СПВ уровня УХД являются ключами к созданию эшелонированной защиты, обладающей средствами эффективного обнаружения нарушителей даже после частичной компрометации системы.

Несмотря на надежность и эффективность СПВ уровня УХД следует отметить, что если нарушитель все же найдет способ компрометации УХД, то есть получит возможность модифицировать существующее и исполнять собственное программное обеспечение, то СПВ может быть нейтрализована. Одним из способов компрометации УХД может быть получение доступа к административной консоли, поэтому ни один клиентский узел не должен обладать информацией, достаточной для административного доступа к УХД. Наличие у нарушителя физического доступа к УХД так же не позволяет полагаться на СПВ, так как нарушитель в таком случае обладает возможностью внесения изменений в программно-аппаратную конфигурацию устройства.

Таким образом, можно выделить следующие основные особенности модели нарушителя, подверженного обнаружению СПВ уровня УХД:

· может располагать полным доступом ко всем устройствам сети, за исключением УХД и их административных консолей;

· может обладать реквизитами доступа легитимных клиентов сети;

· не располагает физическим доступом к УХД.

В работах по обнаружению вторжений для традиционных УХД выделяется четыре базовые категории признаков вторжений, которые могут быть адаптированы к объектно-ориентированой технологии.

1. *Модификация данных и атрибутов*. Среди массива информации, хранимой на УХД, администратор может выделить те данные и метаданные объектов, для которых не ожидаются изменения до тех пор, пока не производится контролируемый процесс обновления системы. К ним могут относиться системные сценарии, исполняемые и конфигурационные файлы, а также другие важные объекты. Выполнение над таким объектом любой OSD-команды, кроме запроса на чтение, может использоваться как триггер события СПВ, ведущего к определенной ответной реакции.

Этот механизм дополняет систему разграничения доступа объектно-ориентированных УХД, поддерживая помимо запрета выполнения операции более сложные виды ответных реакций.

2. *Шаблоны доступа*. Многие приложения оперируют данными согласно определенным шаблонам. Примером может быть работа с протоколами аудита в режиме дополнения с периодической их ротацией [11] или синхронное обновление файлов паролей в UNIX. Любое отклонение от этих шаблонов в отношении заданных объектов может служить признаком аномальной активности.

Большинство вторжений также характеризуются определенными шаблонами собственной активности, например подменой системных утилит или сканированием информации определенного типа. В этом случае наоборот факт воспроизведения шаблона служит основанием для срабатывания СПВ.

Дополнительными источниками сигналов к обнаружению вторжений могут являться любые нетипичные для системы действия, такие как реверсирование времен изменения объектов или их атрибутов, зачастую производимое с целью маскирования признаков вторжения и затруднения диагностики его последствий [12].

В эту же категорию попадают атаки отказа в обслуживании (DoS), демонстрирующие шаблоны доступа с подозрительно высокой интенсивностью использования ресурсов системы. Например, нарушитель может попытаться создать объекты большого размера, занимающие все оставшееся дисковое пространство, или нагрузить систему сложными запросами доступа, исчерпывая ресурсы оперативной памяти и вычислительной мощности. Превышение пороговых значений активности и использования ресурсов в единицу времени может использоваться как признак вторжения. Даже в случае, если срабатывание СПВ оказалось ложным, полученный сигнал послужит для администраторов свидетельством необходимости масштабирования системы.

3. *Нарушение целостности содержимого*. Многие виды объектов обладают структурированным содержимым, для которого могут быть определены правила верификации целостности. При выполнении операций записи или изменения данных они могут быть проверены на соответствие заданному формату. Ввиду высокой ресурсоемкости такой операции применение правил данного типа рекомендуется ограничить наиболее критичными системными объектами.

4. *Подозрительное содержимое*. Если вторжение включает в себя использование вредоносного кода или закладок, то они могут быть немедленно обнаружены СПВ в момент сохранения на УХД. Для этого сохраняемые и изменяемые данные подвергаются сканированию на наличие известных сигнатур. Антивирусная защита на уровне УХД позволяет противодействовать распространению вредоносного кода даже после инфицирования большинства клиентских узлов.

Другими видами подозрительного содержимого являются многочисленные скрытые и пустые объекты, которые могут свидетельствовать о нестандартном использовании системы и попытках нарушения стабильности конкретных приложений посредством замедления операций листинга, поиска и удаления объектов.

Все рассмотренные категории признаков могут быть обнаружены СПВ, основанной на правилах, однако для шаблонов доступа могут дополнительно применяться и поведенческие механизмы обнаружения аномалий с возможностью управления вероятностью ложных срабатываний. Срабатывание правила СПВ может запускать один или несколько различных механизмов ответной реакции и предотвращения вторжений.

Простейшей реакцией является отправка сигнала тревоги через коммуникационный интерфейс УХД в административную систему и фиксация события в локальном журнале аудита. Передаваемая и сохраняемая информация должна содержать идентификатор клиента, время события и полное описание сработавшего правила, включая перечисление выполненных команд, задействованных объектов и переданных данных.

Другим вариантом ответной реакции является искусственная задержка сеанса на определенное время или до тех пор, пока операция не будет подтверждена или запрещена из внешней административной системы. Этот режим позволяет эффективно препятствовать DoS-атакам, атакам перебора и сканированию данных.

В случае если обнаружена опасная операция, например попытка изменения данных аудита или инфицирование объекта, то СПВ может отказать в выполнении такой операции, а также выполнить другие превентивные действия в отношении пользователя от блокировки текущего сеанса до полной блокировки доступа ко всем ресурсам информационной системы.

Выше отмечалась возможность версионного хранения объектов, позволяющая откатывать сеансы клиента для восстановления данных при позднем обнаружении вторжения. Это еще один вариант ответной реакции, которой может обладать СПВ. Несмотря на высокую сложность реализации этого механизма и дополнительные затраты ресурсов [9, 13], такой подход обеспечивает наибольшую устойчивость к факторам нарушения целостности и доступности данных во время вторжений.

Возможны и другие реакции СПВ, например, активация режима максимально подробного аудита всех операций, увеличение периода хранения версионных данных и т. п.

3. Модель системы предотвращения вторжений

Обобщив рассмотренные выше признаки вторжений, можно построить формализованную модель СПВ уровня объектно-ориентированного УХД. Пусть C — множество всех OSD-команд, O — множество всех объектов УХД, V — множество известных СПВ проверок атрибутов OSD-команд, $F \subset V$ — множество проверок форматов сохраняемых данных, $S \subset V$ — множество проверок на наличие в сохраняемых данных сигнатур вредоносного кода. На вход УХД поступают запросы $1, \ldots, t$. Элементарная проверка, выполняемая СПВ для входящего запроса t, заключается в проверке принадлежности команды c_t некоторому подмножеству $C_i \subset C$, объекта o_t подмножеству $O_i \subset O$, и выполнению подмножества проверок $V_i \subset V$ для заданных атрибутов команды a_t:

$$echk_i(c_t, o_t, a_t) = c_t \in C_i \wedge o_t \in O_i \wedge \bigwedge_{v \in V_i} v(a_t).$$

Такие проверки покрывают все выделенные категории признаков вторжения за исключением шаблонов доступа. Для обнаружения шаблонов доступа СПВ должна обладать возможностью сохранения состояния сеанса между запросами клиента. Можно выделить два типа проверок для обнаружения шаблонов доступа:

$$pchk_{i,1}(c_t,o_t,a_t)=echk_{i_{t-n}}(c_{t-n},\ o_{t-n},\ a_{t-n}) \wedge echk_{i_{t-n+1}}(c_{t-n+1},\ o_{t-n+1},\ a_{t-n+1}) \wedge \ldots \wedge echk_{i_t}(c_t,\ o_t,\ a_t),$$

$$pchk_{i,2}(c_t,o_t,a_t)=echk_{i_{t-n}}(c_{t-n},\ o_{t-n},\ a_{t-n}) \wedge echk_{i_{t-n+1}}(c_{t-n+1},\ o_{t-n+1},\ a_{t-n+1}) \wedge \ldots \wedge \neg echk_{i_t}(c_t,\ o_t,\ a_t).$$

Первая проверка позволяет убедиться в соблюдении клиентом некоторого шаблона из $(n+1)$ операции доступа к УХД, а вторая — в его нарушении на $(n+1)$-м шаге. Из нескольких проверок второго типа может быть скомпонована проверка соблюдения клиентом заданного шаблона, то есть отсутствия отклонений от шаблона после совпадения начала последовательности определенной длины. Используемые в последовательностях элементарные проверки зачастую вырожденные, осуществляющие только проверку команды и объекта. Очевидно, что сами элементарные проверки могут рассматриваться как частный случай проверки первого типа при длине последовательности равной 1. Поэтому можно заключить, что указанные два типа проверок охватывают все множество признаков вторжения для СПВ, основанной на правилах, за исключением DoS-атак и других шаблонов доступа, требующих учета временного фактора. Для его учета проверки могут быть обобщены следующим образом:

$$chk_{i,j}(c_t, o_t, a_t) = pchk_{i,j}(c_t, o_t, a_t) \wedge f(\Delta_{t-n+1}, ..., \Delta_t).$$

Здесь “$_{t-n+1}$, …, “$_t$ — интервалы времени между поступлением запросов (t-n, t-n+1), …, (t-1, t), а f — функция проверки временных характеристик шаблона, которая может иметь произвольную форму, накладывающую ограничения на длительность отдельных интервалов, либо на суммарную продолжительность воспроизведения шаблона. Такие проверки позволяют обнаруживать DoS-атаки посредством детектирования длинных цепочек операций определенного рода за ограниченные периоды времени.

Срабатывание каждой из проверок приводит к инициации одной или нескольких ответных реакций из множества, рассмотренного выше. Если обозначить его R, то правила СПВ можно записывать в виде: $rule_i(c_t, o_t, a_t) = if(chk_{i,j_i}(c_t, o_t, a_t), R_i, \varnothing), R_i \subseteq R.$

Для каждого запроса (c_t,o_t,a_t) СПВ последовательно осуществляет обработку заданного администратором множества правил $rule_1$, …, $rule_k$, получает информацию о необходимой ответной реакции и исполняет ее:

$$response(c_t, o_t, a_t) = \bigcup_{i=1}^{k} rule_i(c_t, o_t, a_t).$$

На практике количество занесенных в правила СПВ проверок ограничено, что позволяет сохранять в состоянии сеанса между запросами только информацию, которая может понадобиться для выполнения этих проверок. Это, в частности, означает отсутствие необходимости запоминать результаты всех предыдущих проверок и интервалов времени. Практическая реализация может на каждом шаге для каждой проверки с длиной последовательности большей 1 создавать в памяти СПВ буфер, предназначенный для запоминания состояния выполнения предыдущих элементарных проверок из цепочки. На очередном шаге проверка осуществляется с учетом состояний во всех созданных для нее буферах, которых может быть несколько, если длина последовательности больше 2.

Случай обнаружения DoS-атак может быть оптимизирован путем использования единственного буфера для накопления аддитивных метрик активности клиента в течение сеанса и инициации событий при превышении пороговых значений. Накопительные метрики обнуляются с определенной периодичностью или по срабатыванию события.

Дополнительным механизмом оптимизации работы СПВ может являться выполнение некоторого подмножества проверок в асинхронном режиме, когда операции клиента не блокируются системой и сеанс продолжается, а проверки производятся системой в порядке фоновой очереди. Этот режим рекомендуется использовать только в сочетании с режимом версионности объектов, так как в случае позднего обнаружения вторжения велика вероятность необратимых и дорогостоящих последствий, например, разрушения чувствительной системной информации.

Алгоритмы выполнения элементарных проверок являются широко распространенными в существующих системах защиты информации и сравнительно легко подвергаются оптимизации в среде объектно-ориентированных УХД. Сложные проверки, введенные в представленной модели, представляют собой композиции элементарных проверок и также обладают ограниченной емкостной и вычислительной сложностью. Это позволяет создавать СПВ с высокой эффективностью обнаружения комплексных угроз и минимизированным влиянием на производительность системы при выполнении основных функций, в том числе за счет эффекта ложных срабатываний.

Подводя итог проведенному анализу, можно сформулировать следующие требования к практической реализации СПВ уровня объектно-ориентированных УХД.

· СПВ может быть основанной на правилах или совмещать использование правил с поведенческим анализом, предоставляя возможность управления вероятностью ложных срабатываний.

· Конфигурирование правил СПВ производится только через защищенный административный интерфейс и сохраняется отдельно от пользовательских объектов.

· Возможность создания как глобальных правил, применимых ко всем объектам, так и частных, применимых к конкретным объектам или их группам.

· Допустимые правила должны охватывать все категории признаков вторжений и могут быть представлены следующими проверками:

- выполнение заданной последовательности из одной или более команд;
- нарушение заданной последовательности команд (после совпадения начала последовательности клиент не должен отклоняться от нее до конца);
- нарушение формата сохраняемого/изменяемого объекта;
- обнаружение заданной сигнатуры в данных сохраняемого/изменяемого объекта;
- исчерпание лимита ресурсов, выделенного для клиента.

· Реакция системы при срабатывании правила может быть пассивной или активной, направленной на предотвращение вторжения (отправка сигнала тревоги, искусственная задержка сеанса, отказ в выполнении операции, откат сеанса клиента в случае поддержки версионности).

· Минимизация влияния проверки правил на производительность УХД (в том числе балансирование нагрузки за счет асинхронной проверки правил).

СПВ уровня объектно-ориентированных УХД ввиду их уникальных особенностей могут стать очень эффективным элементом систем комплексной защиты информационных систем предприятий, содержащих объектно-ориентированные системы хранения данных. В частности, они позволяют без существенного влияния на производительность выявлять вторжения в систему даже после компрометации большинства сетевых устройств. При создании промышленных образцов таких СПВ следует уделить особое внимание исследованию характеристик систем правил, которыми они оперируют, с целью создания методологии выбора конфигурации адекватной заданным условиям влияния на производительность и снижения информационных рисков в сети.

СПИСОК ЛИТЕРАТУРЫ:

1. Intrusion Prevention Systems (IPS), NSS Group White Paper. Jan. 2004.
2. *Cheswick B., Bellovin S.* Firewalls and Internet Security: Repelling the Wily Hacker // Addison-Wesley. 1994.
3. *Porras P., Neumann P.* Emerald: Event monitoring enabling responses to anomalous live disturbances // Proc. of National Information Systems Security Conference. 1997.
4. *Banikazemi M., Poff D., Abali B.* Storage-Based Intrusion Detection for Storage Area Networks (SANs) // Proc. of the 22nd IEEE/13th NASA Goddard Conference on Mass Storage Systems and Technologies. 2005.
5. ANSI INCITS 400-2004 — Information Technology — SCSI Object-Based Storage Device Commands (OSD). Dec. 2004.
6. *Pennington A., Strunk J., Griffin J., Soules C., Goodson G., Ganger G.* Storage based intrusion detection: Watching storage activity for suspicious behavior // Proc. of the 12th USENIX Security Symposium. 2003.
7. *Алферов И. Л.* Управление информационными рисками в объектно-ориентированных сетях хранения данных // Безопасность информационных технологий. 2008. № 1.
8. *Sivathanu M., Prabhakaran V., etc.* Semantically-Smart Disk Systems // Proc. of the 2nd USENIX Conference on File and Storage Technologies, San Francisco. CA. Mar. 2003.
9. *Strunk J., Goodson G., Pennington A., Soules C., Ganger G.* Intrusion Detection, Diagnosis, and Recovery with Self-Securing Storage. Carnegie Mellon University Technical Report CMU-CS-02-140. May 2002.
10. *Ganger G., Economou G., Bielski S.* Finding and Containing Enemies Within the Walls with Self-securing Network Interfaces. Carnegie Mellon University Technical Report CMU-CS-03-109. Jan. 2003.
11. *Denning D.* An Intrusion-Detection Model // IEEE Transactions on Software Engineering. Feb. 1987. SE-13(2). P. 222—232.
12. *Farmer D.* What are MACtimes? // Dr. Dobb's Journa. Oct. 2000. 25(10). P. 68—74.
13. *Liu P., Jajodia S., McCollum C.* Intrusion Confinement by Isolation in Information Systems // IFIP Working Conference on Database Security. 2000. P. 3—18.