Раздел II. Защита компьютерных систем

УДК 004.056.5 004.89

А.Ю. Оладько

ПОДСИСТЕМА МОНИТОРИНГА И АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОПЕРАЦИОННОЙ СИСТЕМЕ LINUX

Цель исследования: предложение подхода к проведению аудита информационной безопасности в операционной системе. В рамках данного исследования решены следующие задачи: обоснована необходимость в проведении мониторинга и аудита информационной безопасности, проанализированы адаптивные методы классификации состояний системы. Предложен подход к созданию подсистемы мониторинга и аудита информационной безопасности с применением искусственной иммунной сети. Разработана и описана формальная модель. Предложенная система является адаптивной подсистемой активного аудита построенной на базе искусственной иммунной сети с использованием многоагентного подхода и может применяться как инструмент контроля над состоянием операционной среды и действиями пользователей в операционной системе Linux, а также как элемент более сложных адаптивных самоорганизующихся систем защиты информации в ОС.

Операционная система; искусственная иммунная сеть; адаптивные системы защиты; аудит; мониторинг; информационная безопасность.

A.Yu. Oladko

SUBSYSTEM OF MONITORING AND AUDIT OF INFORMATION SECURITY IN LINUX

The purpose of the study is the proposed approach to the audit of information security in the operating system. The problems solved in the study: substantiates the necessity to monitor and audit security, analyzed adaptive methods classifying system. The approach to create a subsystem for monitoring and audit information security with use of artificial immune network proposed. Formal model developed and described. The proposed system is adaptive active audit subsystem constructed based on artificial immune network using a multi-agent approach and can be used as an instrument of control over the state of the operating environment and the actions of users in the operating system Linux and as part of a complex adaptive self-organizing systems of information security in the OS.

Operating system; an artificial immune network; adaptive security; auditing; monitoring; information security.

Обеспечение безопасности информации в современном бизнесе является одной из ключевых задач. Повсеместное использование персональных компьютеров, автоматизированных рабочих мест пользователей, серверного оборудования и их объединение в локальные, распределённые и глобальные сети на сегодняшний день является необходимым условием для успешной реализации ключевых бизнес-процессов любой организации. Анализ данных статистики, приведенных в работах [1, 2] позволяет сделать вывод о росте числа преступлений, связанных с нарушением основополагающих принципов информационной безопасности: доступности, целостности и конфиденциальности информации. Несмотря на развитие средств защиты, таких как брандмауэры, системы аутентификации и разграничения доступа количество атак злоумышленников на операционные системы (ОС) как одни из ключевых

элементов корпоративных информационных систем организаций возрастает с каждым годом. Увеличение числа атак на ресурсы ОС приводит к необходимости разработки и применения средств и систем защиты способных адаптироваться и проводить свою реконфигурацию в зависимости от состояния операционной среды и событий происходящих в ней. Как правило, способность к адаптации и обучению таких систем защиты обеспечивается за счет использования технологий искусственного интеллекта, анализа данных, модульности и многоагентного подхода. [1–3].

При этом одной из необходимых составляющих адаптивных систем защиты являются подсистемы мониторинга и активного аудита, позволяющие обеспечить сбор статистических данных о событиях, происходящих в ОС, ключевых параметров функционирования ОС и сделать вывод об аномалиях в состоянии, потенциально возможных нарушений происходящих в системе и несоответствии текущего уровня безопасности с допустимым.

Поведение ОС обычно характеризуется дискретными временными рядами наблюдений. При этом проблему обнаружения вторжений и аномалий в поведении ОС можно сформулировать как задачу «разладки», т.е. задачу выявления недопустимых отклонений в характеристиках системы.

Существует несколько методов анализа недопустимых отклонений, включающих в себя: нейронные сети, иммунные сети, статистический анализ, кластерный анализ, поведенческая биометрия.

При применении нейронных сетей в качестве интеллектуального механизма классификации функционирование защищаемой системы и взаимодействующих с ней внешних объектов представляется в виде траекторий в некотором числовом пространстве признаков. В качестве метода обнаружения злоупотреблений, нейронные сети обучаются на примерах атак каждого класса и, в дальнейшем, используются для распознавания принадлежности наблюдаемого поведения одному из классов атак. Основная сложность в использовании нейросетей заключается в корректном построении такого пространства признаков, которое позволило бы разделить классы атак между собой и отделить их от нормального поведения. Нейронные сети для обнаружения аномалий обучаются в течение некоторого периода времени, когда всё наблюдаемое поведение считается нормальным. После обучения нейронная сеть запускается в режиме распознавания. В ситуации, когда во входном потоке не удается распознать нормальное поведение, фиксируется факт атаки. В случае использования репрезентативной обучающей выборки нейронные сети дают хорошую устойчивость в пределах заданной системы; но составление подобной выборки является серьёзной и сложной задачей [4].

Иммунные сети также являются механизмом классификации и строятся по аналогии с иммунной системой живого организма. Анализ литературных источников [2] показывает, что технологии иммунных систем начинают активно применяться в таких областях как принятие решений и управление информационной безопасностью, распознавание образов, диагностика атак и аномальных состояний. Кроме этого, поскольку построение данных систем основывается на биологической иммунной системе, то их явным преимуществом является возможность получения «антител» к неизвестным атакам, что позволит существенно повысить адаптивность механизмов и функций подсистем защиты информации и преодолеть проблемы классических средств обеспечения информационной безопасности. Недавно ученые Лондонского Королевского колледжа сообщили о разработке в рамках проекта The Computational Immunology for Fraud Detection (CIFD) защитной системы для Internet на базе AIS. Предполагается, что на завершение указанного проекта уйдет еще около трех лет. Отличительной особенностью и преимуществом иммунных сетей по данным [6, 7] является возможность их применения для моделирования сложных динамических процессов при этом процесс будет в 3 раза

быстрее, чем традиционными методами, кроме того, обучение искусственных иммунных систем в 40 раз быстрее и распознавание в 1,5 раза безошибочней по сравнению с нейрокомпьютингом.

Методы, построенные на статистическом анализе, используют статистический профиль поведения системы в течение некоторого периода «обучения», при котором поведение системы считается нормальным. Для каждого параметра функционирования системы строится интервал допустимых значений, с использованием некоторого известного закона распределения. Далее, в режиме обнаружения, система оценивает отклонения наблюдаемых значений от значений, полученных во время обучения. Если отклонения превышают некоторые заданные значения, то фиксируется факт аномалии (атаки). Для статистического анализа характерен высокий уровень ложных срабатываний при использовании в локальных сетях, где поведение объектов не имеет гладкого, усреднённого характера [2, 9].

Суть кластерного анализа д состоит в разбиении множества наблюдаемых векторов-свойств системы на кластеры, среди которых выделяют кластеры нормального поведения. В каждом конкретном методе кластерного анализа используется своя метрика, которая позволяет оценивать принадлежность наблюдаемого вектора свойств системы одному из кластеров или выход за границы известных кластеров. Сходен по своей сути со статистическим анализом [5].

Поведенческая биометрия включает в себя методы, не требующие специального оборудования (сканеров сетчатки, отпечатков пальцев), т.е. методы обнаружения атак, основанные на наблюдения клавиатурного почерка и использования мыши. В основе методов лежит гипотеза о различии «почерка» работы с интерфейсами ввода-вывода для различных пользователей. На базе построенного профиля нормального поведения для данного пользователя обнаруживаются отклонения от этого профиля, вызванные попытками других лиц работать с клавиатурой или другими физическими устройствами ввода [9].

На основании методики приведенной в работе [2] данные методы было проведено сравнение описанных выше методов классификации с целью выявления тех, которые наиболее эффективно могут быть применены для решения задачи разработки адаптивной системы защиты в ОС, и в частности при реализации подсистемы мониторинга и активного аудита в ОС Linux. Для проведения анализа был предложен обобщенный показатель оценки (ПАМ), значение которого определяется по следующей формуле (1):

$$П^{AM} = \sum_i K_i \, П_i^{AM}, \tag{1}$$

где Ki – коэффициент относительной важности i-го показателя функциональных возможностей метода – ПАМi, причем Ki удовлетворяет следующему условию нормировки, которое представлено формулой (2):

$$\sum_i K_i = 1, \tag{2}$$

Для сравнения данных методов, на основании типовых свойств и характеристик, а так же требований, которым должна удовлетворять разрабатываемая подсистема защиты, были выделены следующие показатели оценки – ПАМi,:

- способность выявлять аномалии в поведении системы – ПАМ1;
- способность детектировать известные и неизвестные виды атак – ПАМ2;
- способность к обучению – ПАМ3;
- способность подбирать и вырабатывать защитную реакцию в ответ на обнаруженное воздействие – ПАМ4;
- процент ошибочного распознавания – ПАМ5;

- сложность реализации – ПАМ6;
- новизна применения метода в области защиты информации – ПАМ7;

Значение выделенных показателей, задаются по следующему алгоритму:

1. Для показателей с $П^{АМ}_1 – П^{АМ}_4$:
   - показатель принимает значение 1, если функциональные возможности присущи данному адаптивному методу;
   - показатель принимает значение 0,5, если функциональные возможности частично реализованы;
   - показатель принимает значение 0, если такие функции отсутствуют
2. Для показателя $П^{АМ}_5$
   - показатель принимает значение 1, если процент срабатываний у данного метода относительно небольшой;
   - показатель принимает значение 0,5, если данный метод обладает большим процентом ложных срабатываний;
3. Для показателя $П^{АМ}_6$
   - показатель принимает значение 1, если сложность реализации метода средняя;
   - показатель принимает значение 0,5, если данный метод является сложно реализуемым;
4. Для показателя $П^{АМ}_7$
   - показатель принимает значение 1, если данный метод относительно недавно используется для решения задач в области защиты информации и процент его практических реализаций небольшой;
   - показатель принимает значение 0, если данный метод давно и часто применяется в области защиты информации.

Результаты сравнительного анализа адаптивных методов обнаружения атак по выделенным вше показателям представлены в табл. 1.

Таблица 1

Результаты сравнительного анализа адаптивных методов

Адаптивные методы / Показатели – $П^{АМ}_i$	Важность - K_i	Нейронные сети	Иммунные сети	Статический анализ	Кластерный анализ	Поведенческая биометрия
Способность выявлять аномалии в поведении системы	0,1	1	1	1	1	1
Способность детектировать известные и неизвестные виды атак	0,15	1	1	0	0	0
Способность к обучению	0,15	1	1	0,5	0,5	0,5
Способность подбирать и вырабатывать защитную реакцию в ответ на обнаруженное воздействие	0,2	0	1	0	0	0
Процент ошибочного распознавания	0,2	1	1	0,5	0,5	1
Сложность реализации	0,1	1	0,5	1	1	0,5
Новизна применения метода в области защиты информации	0,1	0,5	1	0,5	0,5	1
Сумма		0,75	0,95	0,38	0,38	0,48

По результатам проведенного сравнительного анализа методов с использованием обобщённого показателя оценки анализа можно сделать вывод, что рассмотренные методы: нейронные сети, иммунные сети, статистический анализ, кластерный анализ, поведенческая биометрия являются адаптивными и обладают примерно одинаковой вычислительной сложностью, однако, одной из наиболее развивающихся и перспективных в области диагностики аномалий и выработки решений является технология искусственных иммунных систем (иммунокомпьютинг), которую и предлагается автором использовать при создании подсистемы мониторинга и активного аудита информационной безопасности в ОС.

Для описание подсистемы мониторинга и аудита в ОС Linux предлагается использовать следующий кортеж:

$$SMA=\{\{MAg\}, \{S\}, \{SRec\}, Report, AIS\}, \quad (3)$$

где {Mag} – множество агентов мониторинга, предназначенных для сбора данных о ключевых параметрах описывающих процесс функционирования ОС: характеристики запущенных процессов, информация о пользователях, сетевые соединения и их характеристики, параметры конфигураций модулей ядра ОС; {S} – множество, описывающее состояния системы, формируется на основании данных собранных агентами мониторинга и требований, предъявляемых к безопасности в ОС; {SRec} – множество требований предъявляемых к уровню и показателям безопасности ОС, используется при формировании множества нормальных «безопасных» состояний ОС; Report – отчет о результатах аудита безопасности в ОС, содержит информацию о выявленных несоответствиях между требуемым и текущим состоянием ОС, потенциально возможных нарушениях и рекомендации по их устранению; AIS – искусственная иммунная сеть.

При описании состояний ОС можно выделить: текущее состояние системы $S_{TOS} \in \{S\}$, формирующееся на основании данных собранных агентами мониторинга $MAg_i \in \{MAg\}$ в процессе «реального» времени и множество шаблонов нормальных состояний $\{S_{NOS}\} \subseteq \{S\}$, составленных на основании статистических данных, данных полученных в процессе обучения системы когда все состояния системы считаются условно «безопасными» и требований {SRec} предъявляемых к безопасности ОС. Каждый элемент $S_i \in \{S\}$, описывается следующим кортежем (4):

$$S_i=\{\{PR\}, \{P\}, \{NC\}, \{CM\}\}, \quad (4)$$

где {PR} – множество запущенных процессов в ОС Linux; {P} – множество пользователей ОС: {NC} – множество сетевых соединений; {CM} – множество модулей ядра.

В свою очередь каждый процесс $PR_i \in \{PR\}$, можно представить в виде множество параметров (6):

$$PR = \{UID, PID, \{API\}, \{NCP\}\}, \quad (5)$$

где UID – идентификатор пользователя, запустившего процесс, согласно данному идентификатору определяются права процесса при выполнении API функций операционной системы. Целью злоумышленника является несанкционированное получения UID=0, то есть присвоение процессу прав суперпользователя.

PID – идентификатор процесса в системе. Злоумышленник может использовать различные средства (например, руткиты) для сокрытия подозрительных процессов в системе от контроля администратора. Одним из видов такого сокрытия является временное изменение идентификатора процесса (используется в распространенных руткитах Adore).

{API} – множество API функций операционной системы, которые были вызванны приложением, включая параметры этих вызовов.

{NCP} – множество сетевых соединений, инициированных конкретным приложением.

Далее полученные и сгруппированные в ходе мониторинга данные поступают в искусственную иммунную сеть AIS, которая и производит классификацию состояний системы, полученные на выходе которой данные используются при формировании отчета Report по результатам аудита. Модель иммунной сети с учетом формул (3) и (4) можно представить следующим образом:

$$AIS = (Ag, Ab, d, h, F, ISr), \quad (6)$$

где Ag – множество антигенов, формируется на основании векторов входных значений S_{TOS}; Ab – множество «антител», формируется на основании шаблонов, описывающих нормальные состояния системы $\{S_{NOS}\}$; d – правило вычисления аффинности между антигеном Ag и антителом Ab; h – пороговое значение чувствительности иммунной сети; F – функция классификации системы, F(d,h)=0 если состояние системы классифицируется как «аномальное», F(d,h)=1 если – «нормальное»; ISr – множество, описывающее выявленные несоответствия и параметры, в которых обнаружены расхождения.

Процесс классификации состояний системы в ОС Linux при проведении мониторинга и активного аудита с применением иммунной технологии заключается в следующем:

Формируется множество антител Ab и заполняется значениями из множества S_{NOS}.

Профиль текущего состояния системы S_{TOS} ставится в соответствие с антигеном Ag ($Ag=S_{TOS}$) и антиген Ag сравнивается с элементами $Ab_j \in \{Ab\}$ в качестве меры сравнение применяется метрика $d(Ag, Ab_j)$, представляющая собой аффинность (степень соответствия) между антигеном и антителом. В качестве правила вычисления аффинности могут быть использованы следующие подходы, описанные в табл. 2.

Таблица 2

Правила вычисления аффинностей

Правило r-смежных совпадений	Расстояние по Хэммингу	Евклидово расстояние	Расстояние по Чебышеву
Аффинность равна максимальному числу совпадений в смежных позициях двух шаблонов	Аффинность равна числу совпадающих элементов в одинаковых позициях	Аффинность равна корню квадратному из квадрата разности элементов шаблонов	Аффинность равна наибольшему модулю разности элементов шаблонов

Считается, что S_{TOS} входит во множество нормальных состояний системы $\{S_{NOS}\}$, т.е. система признает данное состояние нормальным и аномалий, а следовательно и попыток вторжения не обнаруживается, если расстояние $d(Ag, Ab_j)$ меньше порогового значения h, $d(Ag, Ab_j) \leq h$, в противном случае система обнаруживает аномалию в поведении и функция F(d,h) принимает значения в соответствии с правилом определенным формулой (7).

$$F(d,h) = \begin{cases} 1, \text{если } d(Ag, Ab_j) \leq h \\ 0, \text{если } d(Ag, Ab_j) > h \end{cases} \quad (7)$$

Далее по полученным результатам подсистема формирует отчет с выявленными несоответствиями текущих параметров системы с «нормальными» значениями параметров в соответствующих им позициях в шаблонах антител и нормальных состояний системы.

Практическая значимость и новизна подсистемы мониторинга и аудита в ОС Linux заключается в том, что предложенная система является адаптивной подсистемой активного аудита построенной на базе искусственной иммунной сети с использованием многоагентного подхода и может применяться как инструмент контроля над состоянием операционной среды и действиями пользователей в системе с целью выявления потенциальных злоумышленников как внутренних так и внешних, так и как элемент более сложных адаптивных самоорганизующихся систем защиты информации в ОС.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Оладько А.Ю.* Модель адаптивной многоагентной системы защиты в ОС Solaris 10 // Известия ЮФУ. Технические науки. – 2011. – № 12 (125). – С. 210-217.
2. *Oladko A. Yu.* Application immune network to create the protection system of OS Solaris 10 // European Science and Technology: international scientific conference.// Bildungszentrum Rdk e.V. Wiesbaden, Germany 2012. – P. 261-266.
3. *Кашаев Т.Р.* Алгоритмы активного аудита информационной системы на основе технологий искусственных иммунных систем: Автореф. дис. … канд. техн. наук. – Уфа, 2008. – 20 с.
4. *Hoffmann G.W.* (2008) Immune Network Theory. Monograph. URL: www.physics.ubc.ca/~hoffmann/ni.html, 2008 г.
5. *Гвозденко А.* Искусственные иммунные системы как средство сетевой самозащиты // ITC Publishing. URL: http://itc.ua/articles/iskusstvennye_immunnye_sistemy_kak_sredstvo_setevoj_samozashhity_4270.
6. *Котов В.Д., Васильев В.И.* Система обнаружения сетевых вторжений на основе механизмов иммунной модели // Известия ЮФУ. Технические науки. – 2011. – № 12 (125). – С. 180-190.
7. *Yoann Vandoorselaere, Laurent Oudot*. Prelude, an Hybrid Open Source Intrusion Detection System // URL: http://www.prelude-ids.org/, 2010.
8. Выбор системы обнаружения атак. URL: http://www.itsecurity.ru, 2007.
9. *Нестерук Ф. Г., Осовецкий Л. Г., Нестерук Г. Ф., Воскресенский С.И.* К моделированию адаптивной системы информационной безопасности // Перспективные информационные технологии и интеллектуальные системы. – 2004. – № 4. – С. 25-31.
10. *Ивахненко А.Г., Савченко Е.А., Ивахненко Г.А., Гергей Т., Надирадзе А.Б., Тоценко В.Г.* Нейрокомпьютеры в информационных и экспертных системах // Нейрокомпьютеры: разработка и применение. – 2003. – № 2.

Статью рекомендовал к опубликованию д.т.н., профессор О.Б. Макаревич.

Оладько Алексей Юрьевич – Волгоградский государственный университет; e-mail: bop-x@yandex.ru; 400062, г. Волгоград, пр-т Университетский, 100; тел.: 88442460368; кафедра информационной безопасности; ассистент.

Oladko Alexey Yuryevich – Volgograd State University; e-mail: bop-x@yandex.ru; 100, University ave, Volgograd , 400062, Russia; phone: +78442460368; the department of Information security; assistant.

УДК 004.056.5, 004.89

А.В. Никишова

ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ МНОГОАГЕНТНОЙ СИСТЕМЫ ОБНАРУЖЕНИЯ АТАК

Была обоснована актуальность задачи обнаружения атак. Были рассмотрены особенности процесса проведения атаки. Были проанализированы действия злоумышленников различных типов на различных этапах атаки. Было показано, какие методы обнаружения атак необходимо применять на различных шагах реализации атак злоумышленником. Была