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

Аткина Владлена Сергеевна
Волгоградский государственный университет.
E-mail: atkina.vladlena@yandex.ru.
400062, г. Волгоград, пр. Университетский, 100.
Тел.: 88442460368.
Кафедра информационной безопасности; ассистент.

Atkina Vladlena Sergeevna
Volgograd State University.
E-mail: atkina.vladlena@yandex.ru.
100, Universitetsky Prospect, Volgograd, 400062, Russia.
Phone: +78442460368.
The Department of Information Security; Assistant.

УДК 004.056.5, 004.89

А.Ю. Оладько

МОДЕЛЬ АДАПТИВНОЙ МНОГОАГЕНТНОЙ СИСТЕМЫ ЗАЩИТЫ В ОПЕРАЦИОННОЙ СИСТЕМЕ SOLARIS 10

Целью исследования является предложение нового подхода к защите информационных систем под управлением операционной системы Solaris 10. Предлагается модель адаптивной системы защиты, построенной на базе многоагентного подхода и технологии искусственных иммунных систем. Задачи, решаемые в исследовании: обоснование возможности применения многоагентного подхода и искусственных иммунных систем для описания и моделирования системы защиты от атак, определение принципов функционирования иммунной системы. Результаты исследования: разработана структура модели и описаны функции иммунной многоагентной системы защиты, описаны принципы инициации первичного и вторичного иммунного ответа; проведено сопоставление элементов иммунной системы человека и элементов операционной системы и системы защиты.

Операционная система; многоагентная система; иммунная система; антиген; иммунный ответ; атака.

A.Yu. Oladko

MODEL OF ADAPTIVE MULTI-AGENT PROTECTION SYSTEMS IN THE SOLARIS 10 OPERATING SYSTEM

The goal of research is to propose a new approach to protect of information systems running Solaris 10 operating system. Model is proposed adaptive protection system built on the basis of multi-agent system and the technology of artificial immune systems. The problems solved in the study: rationale possibility of using multi-agent system and artificial immune systems for describing and modeling the system protection from attacks, the definition of the principles of the immune system. The results of the research are: the structure of the model and describes the functions of immune multi-agent protection system; principles of the initiation of primary and secondary immune response are described; comparison of the elements of the human immune system and elements of the operating system and security are held.

Operating system; multi-agent system; the immune system; antigen; immune response; attack.

Sun Solaris представляет собой мощную и гибкую операционную систему, существующую в вариантах как для процессоров SPARC, так и x86. Solaris предназначается для работы в корпоративных вычислительных сетях и обеспечивает чрезвычайно эффективный и надежный доступ к системам в целом, серверам, базам данных, принтерам и другим сетевым ресурсам.

На сегодняшний день сервера Solaris 10 применяются в различных компаниях для управления своими корпоративными сетями таких, как РосНефть, Национальный Олимпийский комитет, в научно-производственных комплексах федерального значения и т.д. При этом согласно результатам исследования состояния информационной безопасности, опубликованным в 2011 г. в отчете группы X-Force Security компании IBM, из общего количетва найденных уязвимостей в компонентах операционных систем порядка 28 % приходилось на операционную систему Solaris (рис. 1), и хотя в 2010 г. доля Solaris снизилась до 5 %, на момент издание отчета 24 % из них не были закрыты.

Для защиты от атак в операционной системе Solaris постоянно совершенствуются системы защиты, разрабатываются и внедряются новые:

- средства управление службами (Service Management Facility-SMF);
- межсетевой экран IP Filter;
- ролевое управление доступом (RBAC);
- зоны.

В то же время средствами Sun Solaris 10 нельзя защититься от атак, использующих недокументированные возможности, от атак, позволяющих несанкционированно запустить программный код, от атак, использующих недостатки системы хранения или выбора данных об аутентификации, от вредоносного программного обеспечения.

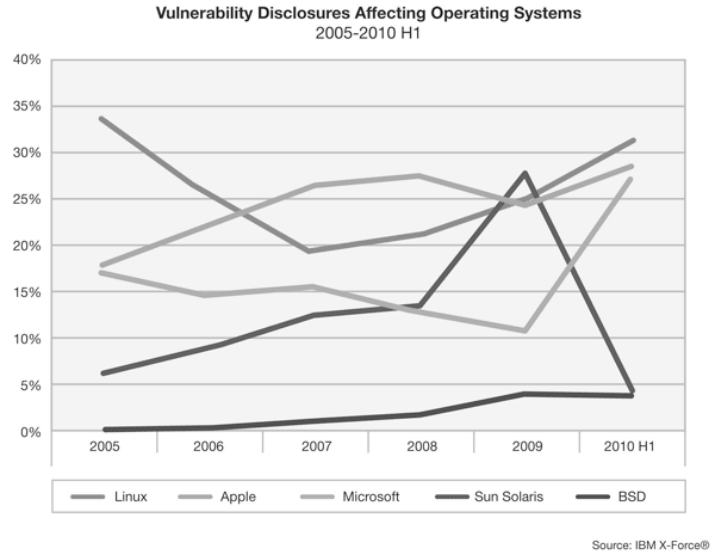

Рис. 1. Статистика уязвимостей, найденных в операционных системах

Также средства Solaris не позволяют защититься от уязвимостей в прикладном программном обеспечении, что приводит к удаленному или локальному выполнению кода (например, ошибка переполнения heap'а и ошибка формата строки). Вследствие этого возникает необходимость в разработке программного комплекса защиты ИС под управлением ОС Solaris 10, в котором были бы реализованы современные инновационные подходы к защите, включая многоагентный и адаптивный подход. Программный комплекс должен обеспечивать возможность распределенного сбора информации, ее интеллектуального анализа, а также быть способным обнаруживать атакующие воздействия, злоумышленную активность в ИС на нескольких уровнях, вплоть до ее локализации, изоляции и устранения, адаптироваться к новым видам атакующих воздействий.

Поскольку разрабатываемая система защиты должна обладать свойствами адаптации к неизвестным злоумышленным воздействиям, то для автоматизации и интеллектуализации процессов защиты предлагается использовать иммунный подход. Это является возможным поскольку можно проследить аналогию и выделить общие функции и принципы функционирования между естественной иммунной системой и системой защиты:

- регистрация, выявление и оценка серьезности событий, имеющих признаки инцидента;
- идентификация инцидента на основе оперативного анализа доказательств, принятие решения в условиях не полной определенности имеющейся информации и при необходимости генерация сигнала тревоги;
- обработка и устранение последствий инцидента путем введения в действие соответствующих ресурсов безопасности [1].

Искусственная иммунная сеть – это адаптивные системы для обработки и анализа данных, которые представляют собой математическую структуру, имитирующую некоторые функции иммунной системы человека и обладающие способностью к обучению, к прогнозированию на основе уже имеющихся временных рядов и принятию решения в незнакомой ситуации. ИИС в принципе не нуждаются в заранее известной модели, а строят ее сами на основе полученной информации в виде временных рядов. Данные системы применяются при решении плохо алгоритмизируемых задач, таких как прогнозирование, классификация и управление [2].

Таким образом, можно построить модель системы защиты на базе иммунной сети, которая будет описываться следующим кортежем:

$$IMSys = (CRI, ANT, X, Y, S, DMF, AGT, ARS, TRS, IRS, PS, MHC, TPS),$$

где CRI – критерии оценки состояния безопасности;

ANT – база знаний об инцидентах;

X – входные воздействия;

Y – реакция на инцидент;

S – состояния системы;

DMF – функция принятия решений (реагирования), которая включает два подэтапа: принятие решения о включении элемента ARS в набор TRS и затем на основании первого подэтапа – принятие решения о включении элемента ARS в набор IRS;

AGT – агенты, т.е. множество программно реализованных мобильных интеллектуальных агентов;

ARS – множество всех доступных для агентов ресурсов безопасности;

TRS – пробные наборы ресурсов, т.е. подмножество ресурсов, которые отбираются для имитационного моделирования, прогноза и адаптации к неизвестному типу инцидента;

IRS – инцидентно-ориентированные наборы ресурсов, т.е. подмножество ресурсов, которыми располагают агенты и которое в совокупности является достаточным для эффективного реагирования на конкретный тип инцидента;

PS – множество процессов системы;

MHC – главный комплекс совместимости – множество профилей, с информацией о типичном поведении процессов;

TPS – множество толерантных процессов.

Разработанная многоагентная система защиты в ОС Solaris 10 имеет архитектуру, представленную на рис. 2.

Поскольку в основе разрабатываемой системы защиты лежит иммунный подход, то все представленные выше агенты, в зависимости от их функционального назначения, условно можно разделить на следующие группы: агенты-реакторы, агенты-рецепторы, агент-координатор, агенты-идентификаторы.

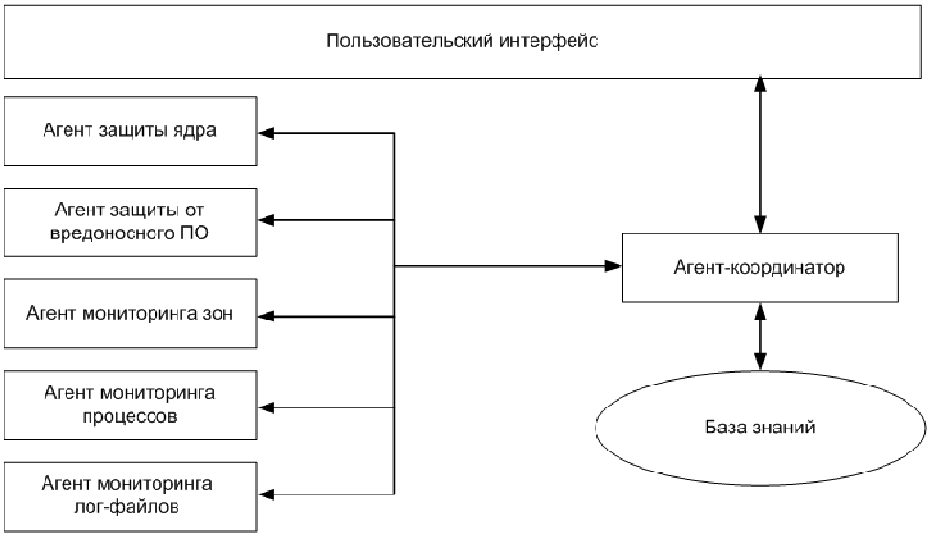

Рис. 2. Архитектура многоагентной защиты в ОС Solaris 10

Соответствующая структура многоагентной иммунной системы защиты представлена на рис. 3.

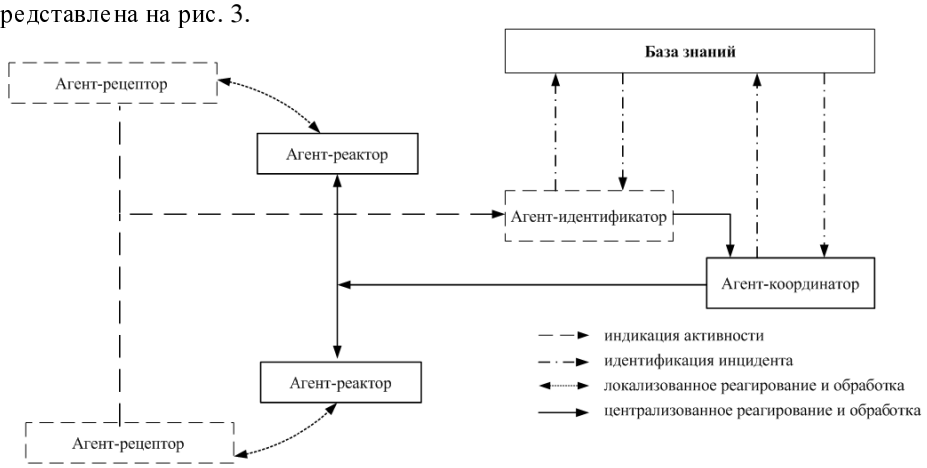

Рис. 3. Структура многоагентной иммунной системы защиты

Агенты-рецепторы соответствуют дендритным клеткам иммунной системы организма и ответственны за выявления нетипичного для данной системы поведения процессов.

База знаний соответствует Т-клеткам памяти. В ней накапливается информация о предыдущих инцидентах безопасности и наиболее эффективных мерах противодействия. Данная информация применяется во вторичном иммунном ответе для быстрейшего подавления злоумышленной активности.

Агент-идентификатор соответствует Т-клеточным рецепторам клеток Т-хелперов и отвечает за идентификацию подмножества процессов, которые являются следствием деятельности злоумышленника. Таким образом, агент-идентификатор в совокупности с базой знаний представляет собой систему обнаружения вторжений (IDS).

Агент-координатор соответствует клеткам Т-координаторам и отвечает за регуляцию интенсивности и продолжительности иммунного ответа. Согласно данным агента-идентификатора и базы знаний подбирает ресурсы безопасности, которые будут задействованы в иммунном ответе, координирует их деятельность, оценивает эффективность иммунного ответа.

Агент-реактор соответствует клеткам Т-киллерам и фагоцитам.

При разработке системы защиты операционной системы Solaris 10 на базе иммунной сети в соответствии клеткам организма были поставлены процессы.

Процесс – это нечто выполняющее программу и создающее среду для ее функционирования. Процесс старается перехватить ресурсы системы, такие как различные устройства или память. Он также запрашивает системные службы, которые выполняются для него и от его имени ядром. Процессы иерархически строго упорядочены. Каждый процесс имеет одного родителя (родительский процесс) и может иметь также одного или нескольких потомков. Иерархия процессов может быть представлена как перевернутое дерево, в вершине которого находится процесс init. Процесс init является первым прикладным процессом, создаваемым во время загрузки системы [3].

При инициировании иммунного ответа важным понятием является понятие антигена. Антигены – генетически чужеродное макромолекулярное вещество (белки, полисахариды и др.) способное индуцировать иммунный ответ [4]. Антигены образуются клетками организма в ходе естественного метаболизма или в результате вирусной или внутриклеточной бактериальной инфекции. В разработанной модели в соответствии естественному метаболизму клеток поставлен результат продуцирования процессов, представленный в виде множества обращений к API-функциям операционной системы.

Каждому структурному состоянию процесса в этом случае будет соответствовать свой вектор $x(t)=(P_1(t), P_2(t),\ldots P_n(t))$, который будем называть геномом поведения процесса, отвечающим за его поведенческие свойства. При этом совокупность геномов поведения процессов, присущих данной системе, образуют главный комплекс совместимости $MHC=\left(x_1(t), x_2(t),\ldots x_k(t)\right)$. Антиген, характеризующий аномальное поведение процесса, представляется в виде $x^A=\left(P_1^A(t), P_2^A(t),\ldots P_n^A(t)\right)$, совокупность антигенов известных иммунной сети и хранимых в клетках памяти определяется следующим образом: $ANT=\left(x_1^A(t), x_2^A(t),\ldots x_m^A(t)\right)$.

Процесс идентификации злоумышленной активности заключается в анализе геномов поведения процессов, на их принадлежность главному комплексу совместимости MHC. Нахождение генома поведения процесса, не входящего в MHC, позволяет идентифицировать атаку. На данном этапе инициируется первичный иммунный ответ, когда иммунная система не располагает данными, какие средства защиты позволяют наиболее эффективно бороться с данной атакой.

Процесс запуска первичного иммунного ответа можно описать следующим образом:

$$\sum x_j(t) \to \overline{x_j}(t), \quad \overline{x_j} \notin MNC.$$

При этом $\overline{x_j}$ включается в множество ANT.

Процедура инициации вторичного иммунного ответа, при котором известны средства защиты, которые позволяют наиболее эффективно бороться с данной атакой, можно описать следующим образом:

$$\sum x_j(t) \to x_j^A(t), \quad x_j^A \in ANT.$$

При этом анализу подвергается как каждый отдельный процесс, так и иерархическое дерево процессов, со всеми процессами-родителями и порожденными ими процессами-потомками. Таким образом, совокупность подозрительных действий процессов-потомков позволяет идентифицировать процесс-родитель как источник этой подозрительной деятельности. Также отдельные подозрительные действия каждого отдельного процесса могут не представляться опасными, при этом их совокупность подозрительных действий множества процессов позволит выявить злоумышленную деятельность в системе. Данная информация накапливается в агенте-идентификаторе и передается агенту-координатору для активации иммунного ответа.

В отношении процессов, идентифицированных как злоумышленные, производится лизис – программируемое разрушение процессов под влиянием агентов-реакторов.

При этом в соответствии с иммунной системой человека, в разработанной системе введено понятие иммунной толерантности: в случае, если какой-либо процесс, важный для функционирования информационной системы, построенной на базе ОС Solaris 10, подвержен уязвимости, которая эксплуатируется злоумышленником, то данный процесс может быть воспринят системой защиты как источник подозрительной активности. При этом лизис данного процесса, проведенный системой защиты, будет означать отказ в доступности необходимого для функционирования информационной системы сервиса. Поэтому для такого процесса вводится иммунная толерантность, т.е. он не разрушается.

Алгоритм функционирования системы защиты на базе иммунной сети будет заключаться в следующем:

1) индикация агентами-рецепторами любой подозрительной активности;

2) распознавание агентами-идентификаторами ненормальной активности как определенного типа антигена при условии нахождения в базе знаний ANT соответствующей сигнатуры или выявление аномалии по отношению к главному комплексу совместимости MHC поведения;

3) получение подсистемой реагирования сигнала от агента-идентификатора об распознавании известного или нового набора антигенов атаки;

4) идентификация атакующего набора угроз инцидента при условии наличия в базе знаний корреляции между характеристиками полученного сигнала об инциденте и записями о наборах атакующих угроз;

5) формирование тестовых наборов механизмов защиты согласно алгоритму, который генерируется агентом-координатором для противодействия новому типу атак (первичный иммунный ответ) либо получение из базы данных набора механизмов защиты для распознанного известного типа атаки (вторичный иммунный ответ);

7) принятие решения относительно выбора инцидентно-ориентированного набора механизмов защиты;

8) выдача подсистемой обработки управляющего сигнала агентам-реакторам относительно обработки инцидента с помощью инцидентно-ориентированного набора механизмов защиты;

9) оценка агентом-координатором эффективности использования инцидентно-ориентированного набора механизмов защиты, примененных против идентифицированного набора антигенов атаки. Пополнение базы знаний новым опытом, анализ инцидента. Занесение в базу знаний информации об эффективности выбранного инцидентно-ориентированного набора механизмов защиты против идентифицированного набора антигенов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Гладыш С.В.* Иммунокомпьютинг в управлении инцидентами информационной безопасности // Искусственный интеллект. – 2008. – № 1. – С. 123-130.
2. *Samigulina G.A., Chebeiko C.B.* Development of immune-networks modeling technology for computers molecular design of medical products // Herald of the National Technical University "KhPI". Subject issue: Information Science and Modelling. – Kharkov: NTU "KhPI". – 2011. – №. 17. – P. 142 – 148.
3. *Вахалия Ю.* Unix изнутри. – СПб.: Питер, 2003. – 844 с.
4. *Игнатов П.Е.* Иммунитет и инфекция. – М.: Время, 2002. – 352 с.

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

Оладько Алексей Юрьевич
Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования Волгоградский государственный университет.
E-mail: bop-x@yandex.ru.
400062, г. Волгоград, пр. Университетский, 100.
Тел.: 88442460368.
Кафедра информационной безопасности; ассистент.

Oladko Alexei Yurievich
Volgograd, State University.
E-mail: bop-x@yandex.ru.
100, Universitetsky Prospect, Volgograd, 400062, Russia.
Phone: +78442460368.
The Department of Information Security; Assistant.