Раздел VI. Информационная безопасность

УДК 681.324

Ю.А. Брюхомицкий

ПРЕДПОСЫЛКИ СОЗДАНИЯ МОДЕЛЕЙ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ НА ПРИНЦИПАХ ФУНКЦИОНИРОВАНИЯ ИММУННЫХ СИСТЕМ

Анализируются предпосылки, условия и ограничения при создании адаптивных моделей компьютерной безопасности, сводящихся к проблеме нахождения отличий «своего» от «чужого». Предлагается расширить применяемую для этих целей модель, основанную на алгоритме отрицательного отбора, путем введения в нее свойств двойной – параметрической и структурной – пластичности. Сформулированы основные принципы параметрической и структурной адаптации в моделях компьютерной безопасности. Результатом моделирования является адаптивная самоорганизующаяся структура, ориентированная на поддержание эффективного уровня обнаружения нарушений компьютерной безопасности при произвольно изменяющихся входных воздействиях.

Защищенные компьютерные системы; адаптивные модели компьютерной безопасности; иммунные системы; алгоритм отрицательного отбора; двойная пластичность; иммунный ответ.

Yu.A. Bryukhomitsky

BACKGROUND OF THE MODELS IN COMPUTER SECURITY PRINCIPLES OF THE IMMUNE SYSTEM

Analyzes the prerequisites, conditions and restrictions when creating adaptive models of computer security, leading to the problem of finding the differences, "a" from "foreign". It is proposed to expand applied for this purpose a model based on negative selection algorithm, by introducing into it the properties of the double – the parametric and structural plasticity. The main principles of parametric and structural adaptation in models of computer security. The result is a simulation of an adaptive self-organizing structure, focused on maintaining an effective level of Computer security violations are detected by arbitrarily changing inputs.

Protected computer systems; adaptive models of computer security; the immune system; negative selection algorithm; double plasticity; immune response.

Назначение системы компьютерной безопасности – обеспечение безопасного функционирования автоматизированной информационной системы, которое реализуется в трех основных аспектах:

- обеспечение конфиденциальности (предотвращение несанкционированного доступа к информации);
- обеспечение целостности (предотвращение несанкционированного изменения информации);
- обеспечение доступности (предотвращение несанкционированного ограничения доступа к информации).

Система компьютерной безопасности является надстройкой к компьютерной системе, и в целом они образуют защищенную компьютерную систему, которая, с точки зрения компьютерной безопасности, функционирует в потенциально враж-

дебной внешней среде. Регулирование взаимоотношений защищенной компьютерной системы с внешней средой определяется принятой политикой безопасности. В случаях выявления нарушений информационной безопасности защищенная компьютерная система предпринимает определенные меры реагирования.

Значительная часть задач, решаемых системами компьютерной безопасности, по своей сути может быть сведена к проблеме нахождения отличий «своего» (легитимных пользователей и процессов, неиспорченных данных, допустимого программного кода, нормальной последовательности системных вызовов и т.п.) от потенциально опасного «чужого» (нелегитимных пользователей и процессов, испорченных данных, зловредного программного кода, ненормальной последовательности системных вызовов и других опасных агентов).

Целью настоящей работы является анализ предпосылок создания адаптивных моделей систем компьютерной безопасности, основанных на принципах функционирования иммунной системы. При этом термин «система компьютерной безопасности» применяется далее только в рамках задач, сводящихся к сформулированной выше проблеме нахождения отличий «своего» от «чужого».

С позиции моделирования защищенной компьютерной системы с помощью механизмов иммунной системы можно выделить три уровня используемых аналогий:

1) защищенная компьютерная система рассматривается как аналог целостного организма;
2) система компьютерной безопасности рассматривается как аналог иммунной системы целостного организма;
3) политика безопасности защищенной компьютерной системы рассматривается как аналог иммунного ответа.

По первым двум уровням обозначенные аналогии являются достаточно прямыми и очевидными. Что касается третьего уровня – аналогии между политикой безопасности и иммунным ответом, то здесь подразумеваются существенные ограничения.

Регулирование взаимоотношений организма с внешней средой в сфере микробиологической безопасности представлено, как известно [1, 2], иммунным ответом, сводящимся к уничтожению или нейтрализации чужеродных клеток. Причем принятие такого решения опосредовано коллективными действиями клеток иммунной системы предположительно без прямого вмешательства нервной системы организма (верхних уровней иерархии). В системах компьютерной безопасности виды реакций на нарушения компьютерной безопасности могут быть существенно различными (например, изоляция или удаление зловредного программного кода, запросы на подтверждение полномочий для определенных действий, закрытие портов, отключение пользователей и т.д.). Причем принятие решения может осуществляться на разных уровнях иерархии: на уровне системы компьютерной безопасности (например, встроенная антивирусная защита), на уровне всей защищенной компьютерной системы (например, запросы на подтверждение полномочий для выполнения определенных действий), а также на более высоких уровнях иерархии управления (например, выдача сообщений администратору, принимающему окончательные решения). По этой причине при моделировании системы компьютерной безопасности на принципах иммунной системы политику безопасности защищенной компьютерной системы условно ограничим простыми реакциями, сводящимися к выдаче сигналов о наличии нарушений компьютерной безопасности.

Применение иммунологического подхода в сфере компьютерной безопасности ограничивается, как правило, наиболее распространенной иммунологической моделью, основанной на алгоритме отрицательного отбора (АОО) [3, 4], который был построен на принципах распознавания «свой – чужой» в системе иммунитета [5]. В самом общем виде он формулируется следующим образом.

1. Определяется понятие «свой», как нормальная динамика поведения системы, которая описывается совокупностью строк символов фиксированной длины. При этом значения данных в строках квантуются по уровням.
2. Создается набор детекторов «произвольных чужих», каждый из которых не должен совпадать с любой строкой нормальной совокупности строк символов «своего». При этом используется правило частичного соответствия, согласно которому две строки совпадают тогда и только тогда, когда они идентичны в определенном числе смежных позиций.
3. При мониторинге новых поступлений данных сначала производится их квантование по уровням в формате, принятом в п. 1, а затем проверка на предмет изменений путем непрерывного сопоставления с детекторами. Активация детектора свидетельствует о появлении измененной строки.

Известные разработки по применению алгоритма отрицательного отбора (АОО) в системах компьютерной безопасности дали интересные и обнадеживающие результаты [3, 6, 7]. Вместе с тем АОО, используемый в системах компьютерной безопасности, в сильно упрощенной форме отражает лишь одну первоначальную стадию сложного процесса формирования иммунного ответа. По существу, первый пункт АОО моделирует принцип сетевого представления исходных данных системы компьютерной безопасности в виде совокупности клеток, подлежащих анализу на предмет чужеродности. Во втором пункте АОО показан принцип формирования детекторов, моделирующий создание в организме иммунокомпетентных клеток (лимфоцитов). Наконец, в третьем пункте АОО путем сопоставления входных данных с детекторами моделируется процесс обнаружения чужеродных данных (антигенов).

Ключевым свойством иммунных сетей, не нашедшим отражения в АОО, является их двойная внутренняя пластичность. Двойная пластичность обеспечивает функционирование иммунной сети в условиях непрерывных возмущений, вызываемых онтогенетическими изменениями организма и его взаимодействием с внешней средой. Двойная пластичность отражает способность иммунной сети к адаптации на основе параметрических и структурных изменений. Термином «параметрическая пластичность» обозначают механизм адаптации, позволяющий системе в ходе выполнения некоторой задачи изменять параметры функционирования для повышения ее эффективности [8].

Двойная пластичность обеспечивает функционирование информационной системы в условиях непрерывных возмущений, вызываемых онтогенезом и внешней средой. Структурная пластичность дает системе новые возможности для адаптации. В системах взаимодействующих элементов структурная пластичность сводится к способности добавления новых элементов и исключения уже имеющихся элементов.

В [9] Ерне на модели иммунной сети показал принцип реализации двойной пластичности, как способ формирования и поддержания памяти для повышения эффективности иммунной реакции при повторном контакте с антигеном:

1. В организме имеется много иммунокомпетентных клеток, циркулирующих по всему телу. Основными из них, участвующими в иммунном ответе, являются лимфоциты (два основных типа Т- и В-лимфоциты). Другие клетки – фагоциты (нейтрофилы, эозинофилы, базофилы и моноциты) – это вспомогательные клетки, обеспечивающие уничтожение или нейтрализацию обнаруженных антигенов.
2. Когда в организме появляется чужеродная клетка – антиген, только малая часть лимфоцитов способна к распознаванию его пептидов (частиц антигена на его поверхности).

3. Такое распознавание стимулирует процессы размножения и дифференцировки лимфоцитов, приводящие к образованию клонов идентичных клеток (антител). Этот процесс размножения клона формирует многочисленную популяцию специфичных к антигену антител.
4. Взаимодействие клона антител с антигеном приводит к уменьшению концентрации и антител, и антигена.
5. Если антигенов, связывающих антитела, становится достаточно много, то это приводит к активации и размножению антител второго типа (анти-антител).
6. Взаимодействие анти-антител с антителами происходит на основе взаимной комплементарности и приводит к уменьшению концентрации антител.
7. Часть оставшихся антител сохраняется для иммунной памяти, что способствует более быстрому иммунному ответу при последующих появлениях похожего антигена.

Принцип обнаружения и нейтрализации чужеродных клеток в иммунной системе поясняет рис. 1.

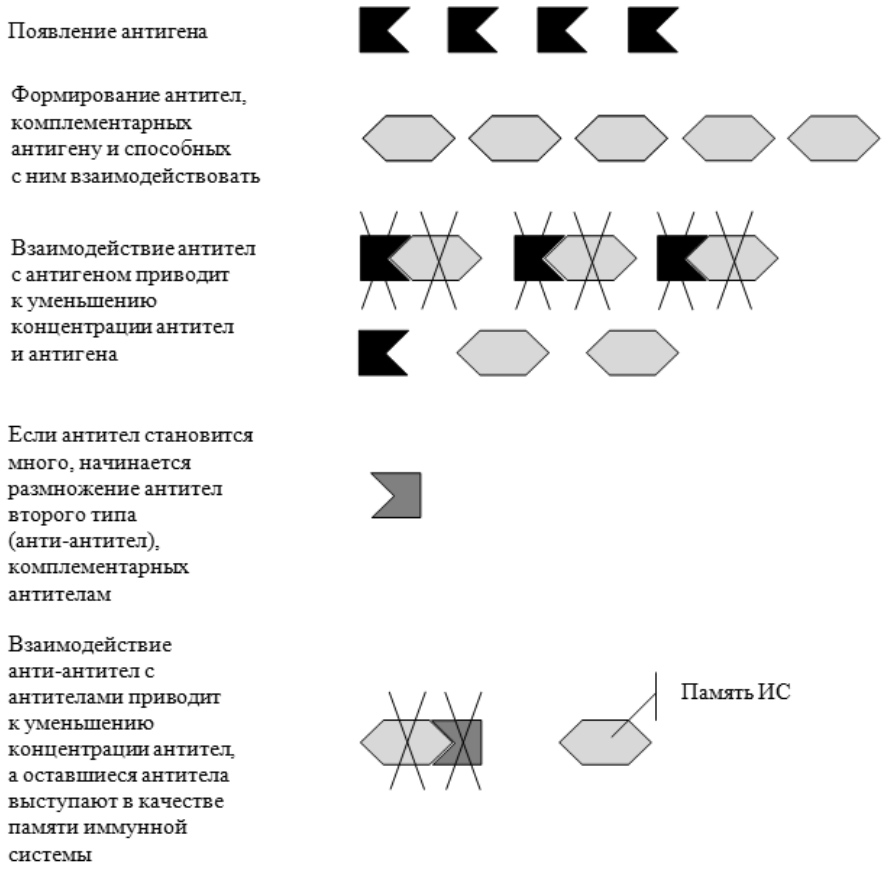

Рис. 1. Процесс обнаружения и нейтрализации чужеродных клеток в иммунной системе

В результате указанных процессов концентрация антител первого типа, необходимых для подавления попавшего в организм антигена, поддерживается на определенном среднем уровне, а формирование памяти порождает процесс образо-

вания нового баланса в сети. Эта разновидность гомеостаза создает устойчивость сети, предохраняет ее от коллапса и неконтролируемого размножения клеток, несмотря на постоянные взаимодействия с внешними и внутренними антигенами.

Приведенная схема иммунного ответа хорошо иллюстрирует основные принципы [1], которым, по всей видимости, должны удовлетворять адаптивные распределенные системы, наделенные свойством двойной пластичности.

Структурные изменения (приток новых антител) происходят реже, чем параметрические изменения (изменение концентрации антител).

Структурные изменения зависят от временной эволюции параметров системы. Приток антител второго типа происходит лишь после того, как концентрация антител первого типа достигает определенного уровня.

Характер структурных изменений определяется сетевыми взаимодействиями, а не только внешними факторами.

Вновь добавляемые элементы комплементарны, а не подобны уже имеющимся.

Из рассмотрения модели функционирования иммунной сети следует важный вывод: за достижение полезного результата отвечает коллективное поведение системы, а не ее взаимодействие с внешней средой [1].

Нетрудно заметить также, что даже в сильно упрощенном виде, процесс обнаружения и нейтрализации чужеродных клеток в иммунной системе гораздо сложнее, чем модель на основе АОО. Это оправдывает попытку использовать и отразить указанные важные свойства иммунной сети в соответствующих моделях систем компьютерной безопасности для придания последним свойств адаптивности в условиях высокой динамики взаимодействия с потенциально опасным внешним окружением.

Свойство двойной пластичности иммунных сетей позволяет сформулировать основные принципы параметрической и структурной адаптации при их моделировании в системах компьютерной безопасности:

1. Масштаб времени структурной адаптации должен быть больше масштаба времени параметрической адаптации.
2. Структурные изменения должны определяться динамикой изменения параметров системы, обусловленных внутрисистемными процессами, и не зависеть от внешних факторов.
3. Структурные изменения должны отражаться в количественных характеристиках системы, отражающих коллективные действия элементов.

С условием принятого выше ограничения по способу реагирования на «чужих» модифицированный АОО, отражающий две стадии пластичности, свойственные иммунной системе, в упрощенном виде можно отразить следующей схемой.

1. Первоначальная конфигурация системы компьютерной безопасности, как модели иммунной системы, создается на основе АОО [1, 3], после чего она включается в режим функционирования.
2. В процессе функционирования системы компьютерной безопасности будут возникать события, состоящие в появлении строк входного сигнала, отмеченных в памяти системы как «чужие» (антиген). Эти события вызовут активирование определенных детекторов (антитела).
3. Активировавшиеся детекторы размножаются с сохранением аффинности со строками входного сигнала, вызвавшими их срабатывание. Например, в строке входного сигнала появилось сочетание значений 10 15 20, вызвавшее срабатывание детектора вида 8 14 5 10 15 20 13 2. Это сочетание значений используется как скользящее окно в строке символов детектора. При этом остальные позиции строки заполняются случайно в заданном диапазоне значений. Тем самым, генерируются новые – вторичные детек-

торы, в которых используется то же сочетание 10 15 20, но размещается оно в разных смежных позициях. Например:

8 14 5 10 15 20 13 2;

11 6 10 15 20 19 9 12;

4 10 15 20 7 16 19 10;

18 19 5 2 15 10 15 20 и т.д.

Вторичные детекторы в процессе генерации, как и первичные, проверяются на частичное соответствие с эталоном «своего». Вторичные детекторы, для которых такое соответствие обнаруживается, уничтожаются. Оставшиеся вторичные детекторы пополняют набор первичных детекторов. Число генерируемых вторичных детекторов автоматически регулируется заданным числом вторичных детекторов, оставшихся после проверки, на частичное соответствие с эталоном «своего». Оставшиеся вторичные детекторы с позиции моделирования иммунной системы играют роль антител, комплементарных к строкам входного сигнала, принадлежащих “чужому” (антигену).

1. Вторичные детекторы по мере их появления, наряду с первичными, включаются в процесс анализа входного сигнала и способствуют повышению эффективности распознавания «чужого», вызвавшего их появление. При повторном появлении «чужого» с близкими параметрами вторичные детекторы будут играть роль памяти системы компьютерной безопасности на данный вид ее нарушения.
2. Констатация факта предполагаемого нарушения компьютерной безопасности и соответствующая реакция системы компьютерной безопасности формируется как вероятностная величина по совокупности откликов всех детекторов (как первичных, так и вторичных).
3. Непрерывное создание вторичных детекторов для разных «чужих» будет неизбежно приводить к неограниченному росту общего числа детекторов. Для поддержания баланса детекторов на заданном уровне необходим какой-то механизм их регулирования. Используя аналогии с нервной и иммунной системами, можно, например, встроить механизм определения первичных детекторов, которые ни разу не активировались в процессе анализа входного сигнала, и уничтожать их в количестве, пропорциональном количеству включаемых вторичных детекторов. В такой механизм целесообразно также ввести функцию забывания, которая будет выбирать кандидатов на уничтожение по значению периода времени, прошедшего после их последней активации.

Все этапы указанного процесса реализуются параллельно и являются составными фазами рабочего режима системы компьютерной безопасности. То есть традиционные для подобных систем этапы обучения и рабочего функционирования здесь органично взаимосвязаны между собой и регулируются внутренними коллективными взаимодействиями элементов, лишь опосредованно стимулируемыми внешним окружением.

Система компьютерной безопасности, созданная по описанной схеме, будет представлять собой адаптивную самоорганизующуюся структуру, ориентированную на поддержание эффективного уровня обнаружения нарушений компьютерной безопасности в условиях произвольно изменяющихся внутренних состояний информационной системы и внешних воздействий.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Искусственные иммунные системы и их применение / Под ред. Д. Дасгупты; Пер. с англ. под ред. А.А. Романюхи. – М.: Физматлит, 2006. – 344 с.
2. *Kuby J.* Immunology. W.H. Freeman and Co., 2nd edition, 1994.
3. *Forrest S., Perelson A.S., Allen L., Cherukuri R.* Self-nonself discrimination in a computer // In: Proc. of IEEE symposium on research in security, Oakland, CA, 16-18 May, 1994. – P. 202-212.
4. *Dasgupta D., Forrest S.* Tool breakage detection in milling operations using a negative-selection algorithm // Technical report CS95-5, Department of computer science, University of New Mexico, 1995.
5. *Percus J.K., Percus O., Perelson A.S.* Predicting the size of the antibody combining region from consideration of efficient self/non-self discrimination // PNAS. – 1993. – Vol. 60. – P. 1691-1695.
6. *D'haeseleer P., Forrest S., Helman P.* An immunological approach to change detection: algorithms, analysis, and implications // In: Proc. of Ieee symposium on research in security, Oakland, CA, May, 1996.
7. *Forrest S., Hofmeyr S.A. Somayaji A., Longstaff T.A.* A sense of self for unix processes // In: Proc. Of IEEE symposium on research in security and privacy, Oakland, CA, May, 1996.
8. *Bersini H., Varela F.* The immune learning mechanisms: Recruitment reinforcement and their applications // Computing with biological metaphors (Ed/ R/ Patton). – L.: Chapman and Hall, 1994.
9. *Jerne N.K.* Towards a network theory of the immune system // Ann. Immunol. (Inst/ Pasteur). – 1974. – Vol. 125. – P. 435-441.

Статью рекомендовал к опубликованию к.т.н. М.Ю. Руденко.

Брюхомицкий Юрий Анатольевич – Технологический институт федерального государственного автономного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге; e-mail: bya@tsure.ru; 347928, г. Таганрог, ул. Чехова, 2; тел.: 88634371905; кафедра безопасности информационных технологий; доцент.

Bryukhomitsky Yuriy Anatoly – Taganrog Institute of Technology – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education "Southern Federal University"; e-mail: bya@tsure.ru; 2, Chekhov street, Taganrog, 347928, Russia; phone: +78634371905; the department of security in data processing technologies; associate professor.

УДК 004.056; 004.8

Е.С. Абрамов, А.В. Андреев, Д.В. Мордвин

ПРИМЕНЕНИЕ ГРАФОВ АТАК ДЛЯ МОДЕЛИРОВАНИЯ ВРЕДОНОСНЫХ СЕТЕВЫХ ВОЗДЕЙСТВИЙ

Использование графов атак при проведении анализа защищённости позволяет учесть взаимосвязи отдельных узлов и их параметры защищенности, что даёт более точные данные для оценки защищенности всей системы в целом, чем при исследовании свойств защищенности отдельных узлов.

Эта статья описывает процесс расчета графа атак, анализ полученных результатов и оценку эффективности существующих контрмер.

Модель сети уточнена до уровня сервисов, а не пары <интерфейс-порт>. В модели учтены динамическая маршрутизация и фильтрация на любом сетевом объекте, NAT, состояния в графе атак детализированы до триады <конфиденциальность, целостность, доступность>. При построении графа атак учитываются и локальные, и сетевые уязвимости.

Представлены результаты экспериментальной оценки производительности системы. Для анализа 10 000 моделируемых хостов потребовалось в среднем около 100 секунд.