УДК 004.056

Метод построения моделей безопасности компьютерных систем

Виктор АЛЕКСЕЕВ

Алексеев Виктор Михайлович *– доктор технических наук, профессор кафедры «Управление и защита информации» Московского государственного университета путей сообщения (МИИТ), Москва, Россия.*

Viktor M. ALEKSEEV

Method of Constructing Security Models of Computer Systems

(текст статьи на англ. яз. – English text of the article – p. 20)

В статье рассматриваются вопросы, связанные с построением систем мониторинга, обеспечивающих выявление угроз в информационной среде. В частности, метод распознавания для реализации моделей анализаторов в зоне заданного пространства доверенных и возможных недоверенных маршрутов движения информации.

Ключевые слова: информационный поток, решающие правила, анализатор угроз, доверенные и недоверенные маршруты, информационная безопасность, изолированная программная среда, скрытые каналы, мониторинг субъектов.

Актуальность проблем построения модели информационной безопасности очевидна. Множество публикаций посвящено этому вопросу. Идёт постоянная борьба между компаниями, защищающими свои интеллектуальные разработки, группами лиц, пытающихся нечестными методами завладеть ими. Поскольку хранение данных, обмен информацией осуществляются с использованием сетевых технологий, то возникает возможность кражи критически важной информации. Подвержены информационным атакам и объекты государственной инфраструктуры, включая принадлежащие транспортной отрасли.

В этом контексте ставится задача обосновать и оценить применение методов распознавания для реализации моделей анализаторов угроз. Суть подхода состоит в том, что любой процесс зарождения информации и её передачи по вычислительной сети должен быть строго регламентирован. Проблема же заключается в реализации системы, распознающей доверенные маршруты в информационной системе по набору различных признаков. Обучение подобной системы может проходить с учителем или без такового.

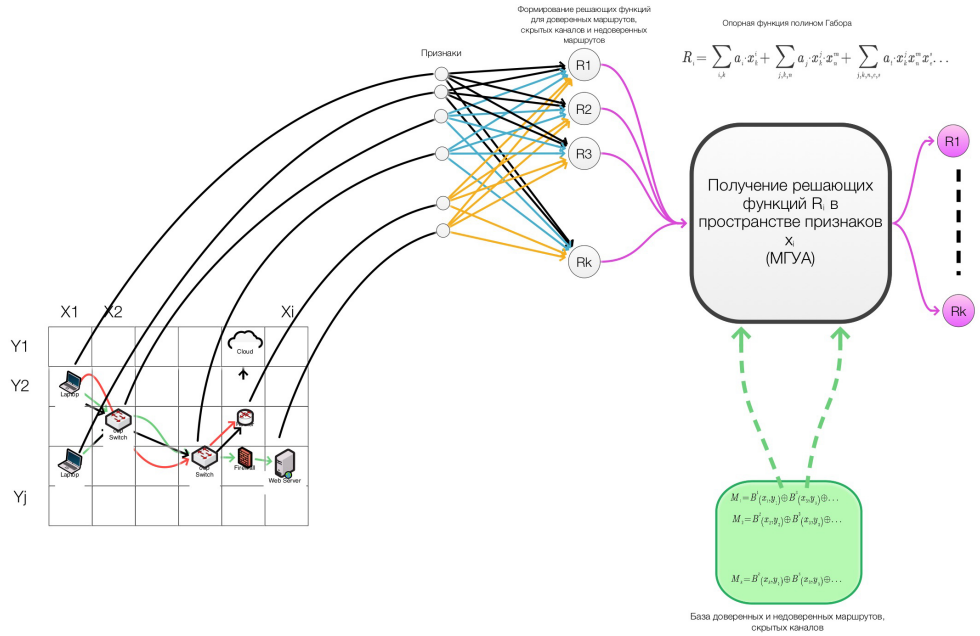

Рис. 1. Построение решающих правил.

В нашем случае описывается подход к решению классической задачи распознавания с использованием заданного пространства доверенных и возможных недоверенных маршрутов. Решающие правила, обеспечивающие распознавание правильности движения информации по доверенным маршрутам, должны строиться на использовании регламентирующих документов той организации, для которой система реализуется.

Распознающие системы работают только на основе признаков. Пространство признаков формируется с использованием встроенных агентов, которые устанавливаются на объекты сетевой инфраструктуры: коммутаторы, точки доступа, маршрутизаторы, защитные экраны, серверы и персональные компьютеры.

Признаки формируются с учетом:

– числовых параметров (количество переданных данных по различным протоколам, загрузка центрального процессора, число файлов и так далее);

– категориальных параметров (типы протоколов, имена файлов, открытые порты и др.);

– нестандартных параметров (время задержки пакета, хеш отпечатки логина и пароля, биометрические параметры и т.п.).

На основе распорядительных документов по безопасности для каждого подразделения устанавливаются доверенные маршруты в информационной системе, которые определяют движение информации.

Для реализации модели предложено использовать координаты объектов сетевой инфраструктуры, задаваемых в виде координатной модели. Этот принцип позволяет перейти к описанию с использованием числовых координат вместо буквенных значений объектов или субъектов. Открываются новые возможности для внесения дополнительных объектов в модель (например, идентификации скрытых каналов утечки информации), расширения функциональности информационной системы (скажем, создания специальных аппаратных средств хранения информации), а также при реконструкции инфраструктуры информационной системы (изменении сетевой структуры предприятия).

База решающих правил в распознающей системе осуществляется на основе построения модели, состоящей из объектов, субъектов и граф, соединяющих их. Полученные решающие правила представляют наборы цепочек, по которым движется информация в контролируемой системе. Причём каждый объект имеет определенные координаты, присвоенные ему в координатной модели. Как было отмечено выше, решающие правила должны формироваться на основе различных признаков: разрешённые протоколы, порты, признак аутентификации (из сервера kerberos, биометрические признаки) и признаки координаты объектов сети, по которым движется информация, а также геоинформационные признаки субъектов, допущенных в систему. Каждый признак имеет присвоенный числовой эквивалент.

Решающие правила определяют доверенные маршруты движения информации по вычислительной сети. При этом могут возникнуть случаи:

– потери информации, обусловленные возникновением очередей на объектах (коммутаторах, маршрутизаторах, точках доступа);

– незаконного направления информации по недоверенному маршруту (субъект пытается незаконно отправить информацию);

– скрытые каналы передачи информации (установленные легально приложения отправляют персональные данные с рабочих мест компьютеров пользователей).

Рассмотрим методы получения решающих правил. Получение решающих правил является наиболее ответственным шагом в реализации модели безопасности контролируемой системы. Получение таких правил осуществляется с использованием метода самоорганизации – группового учёта аргументов [1]. На рис. 1 приведена графическая интерпретация метода при наличии многорядного перцептрона. В системе рассматриваются возможные варианты движения информации, прописанные в распорядительных документах (база доверенных и недоверенных маршрутов, скрытых каналов). Здесь же случаи, связанные с потерей информации, недоверенными маршрутами, скрытыми каналами, другие варианты утечки.

В реализации решающих правил участвуют геоинформационные признаки субъектов и объектов, которые могут быть допущены к работе в системе. Вся сеть представлена сеточной моделью, на которой определены координаты установки объектов (коммутаторов, маршрутизаторов, серверов и другого оборудования). Причём детализация сети обуславливает глубину анализа возникновения угрозы в сети. Решающие правила представляют лингвистические цепочки, построенные по модели сетевой структуры.

В качестве опорной функции выбран полином Габора:

$$R = \sum_{i,k} a_i \times x_k^i + \sum_{j,k,n,m} a_j \times x_k^j \times x_n^m + \sum_{j,k,n,m,e,s} a_j \times x_k^j \times x_n^m \times x_e^s. \quad (1)$$

Центральные состояния объектов, включённых в базу маршрутов, также участвуют в получении решающих правил. Считаем, что при правильной реализации маршрута пакет не отклоняется от заданного маршрута и движется по одному из маршрутов, заданных в базе. В этом случае реализуется последовательный маршрут движения информации с участием соответствующих объектов. На каждом объекте B_i должно проверяться соответствие информации, содержащейся в пакете, заданному маршруту. Реализовать данное условие в решающей функции можно с применением полинома Габора. Расчёт значений коэффициентов проводится на многорядном перцептроне. Пусть x_{i+1} и центральное значение равно 1. Центральное значение для признака x_{i+1} формируется из базы доверенных маршрутов. Из полинома Габора для двух признаков x_i и x_{i+1} следует:

$$R = a_0 \times x_i + a_1 \times x_{i+1} + a_2 \times x_i \times x_{i+1} + a_3 \times x_i^2 + a_4 \times x_{i+1}^2 + \ldots + . \quad (2)$$

Члены в уравнении (2) с коэффициентами a_2, a_3 и a_4 представляют квадрат разности

$$R = (x_i - x_{i+1})^2, \quad (3)$$

при определенных значениях коэффициентов.

Признак x_i принимает одно из значений из множества $M_{\text{пр}}$ (соответствие числового значения 0 – протокол http, 1 – dhcp, 2 – sip и так далее). Признак x_i формируется с помощью агентов, установленных на объектах. Выход R и значения признаков приведены в таблице 1.

Подставляем значения признаков и выхода модели в уравнение (2), получаем переопределенную систему, которую решаем по методу Гаусса [1,2] для переопределенных систем уравнений:

$$[a_k]=[R]\times[x_{ij}]^T\times\left([x_{ij}]\times[x_{ij}]^T\right)^{-1}. \quad (4)$$

В случае формирования маршрута на объекте с дополнительными признаками общее описание полинома Габора будет иметь вид:

$$R=a_0\times x_i+a_1\times x_{i+1}+a_2\times x_i\times x_{i+1}+a_3\times x_i^2+$$
$$+a_4\times x_{i+1}^2+a_5\times x_j^2+a_6\times x_{j+1}^2+a_7\times x_j\times x_{j+1}. \quad (5)$$

Из приведённой формулы (5) следует, что для двух признаков решающие правила будут иметь вид:

$$R=(x_i-x_{i+1})^2+(x_j-x_{j+1})^2. \quad (6)$$

Для каждого объекта B_i строятся решающие правила R_i в соответствии с заданным доверенным маршрутом. Если в маршруте участвуют несколько объектов B_i, то соответственно все решающие правила формируются в единое, описывающее прохождение пакета

$$R_{B1}=\sum_i\left(x_i-x_{i,B1}^*\right)^2, \text{ для объекта } B_1, \quad (7)$$

$$R_{B2}=\sum_i\left(x_i-x_{i,B2}^*\right)^2, \text{ для объекта } B_2, \quad (8)$$

$$R_{Bj}=\sum_i\left(x_i-x_{i,Bj}^*\right)^2, \text{ для объекта } B_j \quad (9)$$

и преобразуются в формулу для доверенного маршрута M_k:

$$R_{M_k}=\sum_i\left(x_i-x_{i,B1}^*\right)^2+\sum_i\left(x_i-x_{i,B2}^*\right)^2+\ldots$$
$$+\sum_i\left(x_i-x_{i,Bj}^*\right)^2, \quad (10)$$

где $i = 1, n$ – набор заданных признаков в системе мониторинга, формируемый агентами.

Определение принадлежности реального информационного потока к одному из решающих правил проходит в реальном масштабе времени путём сбора информации от встроенных агентов в объекты инфраструктуры (см. рис. 2). Сеть мониторинга информации виртуально отделена от контролируемой сети и должна отвечать требованиям леммы (базовая теорема изолированной программной среды ИПС) [3, 4].

Таблица 1

Значения выходов R и признаков

X_i	X_{i+1}	$R_{\text{выход}}$
0	1	1
1	1	0
2	1	1
3	1	4
4	1	9
5	1	16

Лемма. Если с момента времени t_0 в ИПС действует только порождение субъектов с контролем неизменности объекта-источника и все порождения абсолютно корректны относительно друг друга, как и существование субъектов (включая мониторинг безопасности объектов и субъектов), то в любой момент времени $t>t_0$, программная среда остается ИПС.

По условию леммы в программной среде возможно существование потоков, изменяющих состояние объектов, не ассоциированных в этот момент времени с каким-то субъектом. Если объект с измененным состоянием не является источником для порождения субъекта, то множество субъектов ИПС не расширяемо, в противном случае (измененный объект является источником для порождения субъекта) по условию теоремы (порождение субъекта с контролем) порождение субъекта невозможно. Таким образом, в любой момент времени $t>t_0$, программная среда остаётся средой ИПС. Возникновение информационного потока производится субъектом путем инициализации приложения, которое связывается по заданному протоколу с сервером приложения. Для технической реализации модели мониторинга безопасности требуется:

• соблюдение условий корректности субъектов путём использования виртуальной части в локальной сети VLAN,

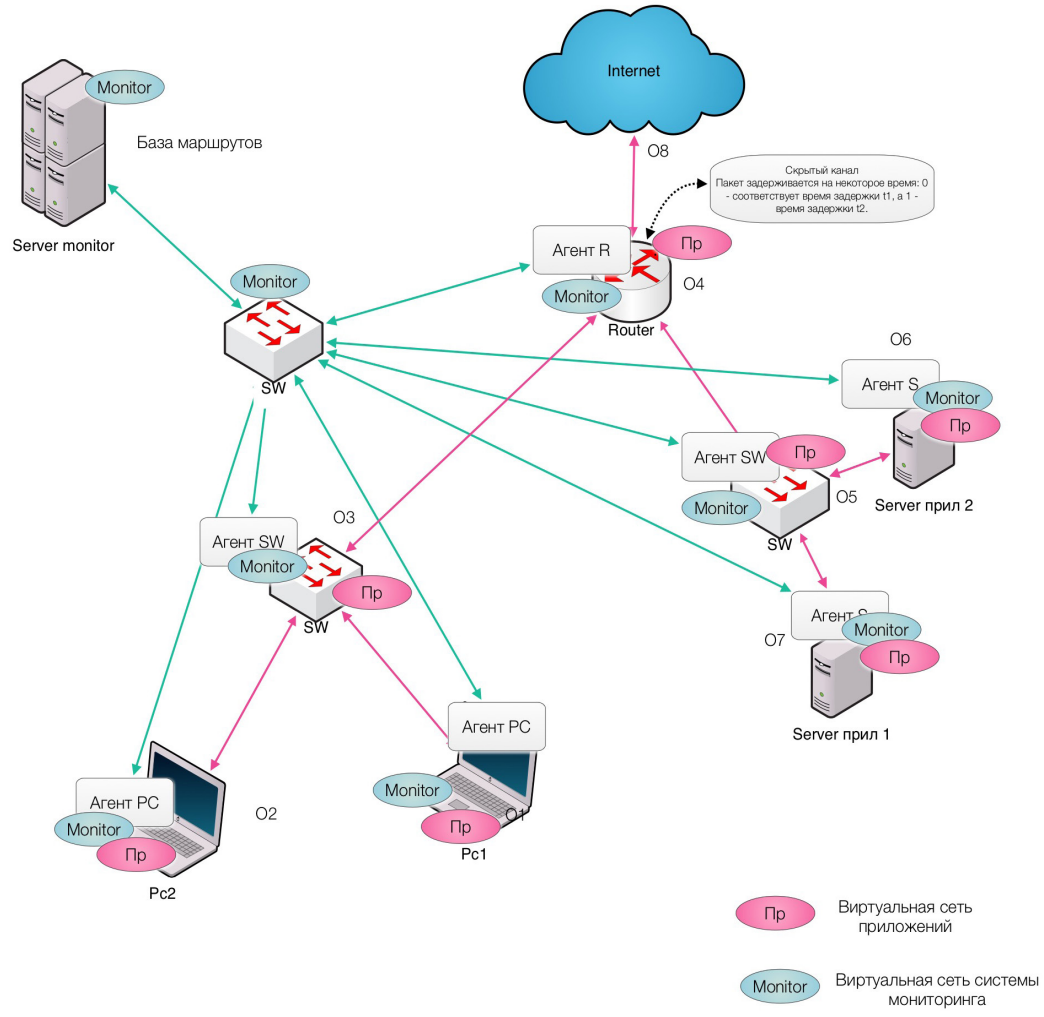

Рис. 2. Сеть мониторинга (ИПС) со встроенными агентами.

разделением ресурсов: объектов и субъектов внутри сети, а во внешней среде использованием VPN (протокол ip-sec);

• монотонность выполнения правил – неизменение правил выполнения функциональности приложений в сети;

• реализация мониторинга безопасности объектов и субъектов с обязательным использованием признаков прохождения идентификации с помощью средств, встроенных в ОС.

Обработка должна проходить по каждой модели объекта B_i по мере продвижения пакета. Наиболее сложный момент связан с потерей пакета или его постановкой в очередь, при перегрузке коммутатора и применении модели редукции произвольно выбранных пакетов, то есть удаления. В этом случае пакет теряется, а следовательно, решающее правило даст результат, что пакет не следует ни по одному из доверенных маршрутов. И значит, нужно включить решающие правила, которые будут отражать данную специфику сети. Буферизация пакетов работает на всех коммутаторах, маршрутизаторах, защитных экранах и других сетевых устройствах. Пакет может быть удалён или задержан на время пропуска приоритетных. То есть необходимо некоторое время на отслеживание пакета, а это требует «фиксации» решающего правила, отслеживающего некоторый доверенный маршрут после поступления на объект сетевой инфраструктуры.

Случай возникновения скрытых каналов отличается тем, что пакет начинает движение по доверенному маршруту (см. рис. 2). Но особенность заключается в том, что пакет задерживается на некоторое время: 0 – время задержки t_1, а 1 – время задержки t_2. Агент скрытого канала производит задержку, на первый взгляд безобидную, тем самым передавая секретную информацию. Как правило, это осуществляется на конечном устройстве маршрутизатора, что ещё раз показывает, что анализаторы должны содержать модель, позволяющую отслеживать временные задержки.

Пакет поступает на сформированные правила контроля доверенных маршрутов в сети, недоверенных маршрутов и скрытых каналов. Признаки, сформированные агентами, поступают на все множество решающих правил. Агенты формируют пространство признаков пакета в сети, которые поступают в решающие правила. Решающие правила дают значения, формируемые в зависимости от пути следования пакетов:

– агент объекта 1: признаки x_i –> решающие правила объекта 1 всех маршрутов;

– агент объекта 2: признаки x_i –> решающие правила объекта 2 всех маршрутов;

– агент объекта n: признаки x_i –> решающие правила объекта n всех маршрутов.

Решающее правило, принимающее минимальное значение или равное нулю, показывает, какой маршрут проходит данный пакет, сформированный приложением P_{ri}. Происходит сравнение маршрута пакета с доверенным маршрутом приложения P_{ri}. Если значение R_{Mk} равно нулю и совпадает с заданным значением в базе решающих правил, то угрозы нет. В случае неравенства $R_{Mk} \neq 0$ ищутся решающие правила с минимальным числовым значением, далее сравниваются с базовыми маршрутами M и делается вывод о возникновении или отсутствии угрозы под индексом j:

$$min\left(R_{M_k}\right) \rightarrow \forall k, \left(R_{M_k} \rightarrow M_j\right); j \in \{1,k\}. \quad (11)$$

Процесс правильности работы решающих правил оценивается достоверностью контроля P_d и зависит от ошибок первого P_1 и второго рода P_2, обусловленными возникающими неточностями при формировании признаков агентами на объектах из-за программных ошибок и других факторов. Достоверность определяется формулой: $P_d = 1 - P_1 - P_2$.

ВЫВОДЫ

Применение методов распознавания угроз при реализации моделей безопасности является прорывным направлением с точки зрения информационной безопасности в компьютерных системах. Присутствие координатной модели в процессе создания инфраструктуры, обеспечивающей использование в решающих правилах числовых координат объектов и субъектов, даёт возможность к появлению доверенных маршрутов движения информации, а также формализации скрытых каналов передачи, недоверенных каналов передачи информации и других новых аспектов на уровне сетевого взаимодействия.

Существенным преимуществом подхода становится то, что при этом не требуется больших вычислительных мощностей, легче реализовать системы, работающие в реальном масштабе времени и управляющие процессами передачи информации, повысить уровень безопасности и предотвращения утечки информации.

ЛИТЕРАТУРА

1. Ивахненко А. Г. Принятие решений на основе самоорганизации. – М.: Советское радио, 1976. – 325 с.

2. Ивахненко А. Г. Индуктивный метод самоорганизации моделей сложных систем. – Киев: Наукова думка, 1982. – 246 с.

3. Девянин П. Н. Модели безопасности компьютерных систем. – М.: Горячая линия-Телеком, 2013. – 338 с.

4. Алексеев В. М., Алексеев В. В. Модель информационного взаимодействия сервисов в ИТ-системе высокоскоростного транспорта // Транспорт Урала. – 2012. – № 3. – С. 43–48.

Координаты автора: **Алексеев В. М.** – avm@niit-miit.ru.

Статья поступила в редакцию 03.10.2016, принята к публикации 22.12.2016.