Предложенная в работе модель позволяет выполнять поэтапное моделирование атаки для различных компьютерных систем. Одним из достоинств данной модели является то, что использование общей памяти не нарушает концепции автоматного моделирования, поскольку как уже отмечалось общая память является аргументом только для формирования функции выходов. Приведенные соображения позволяют предположить, что для данного типа автоматов может быть разработана алгебра, позволяющая производить над автоматами наборы действий.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Schneier B.* Attack Trees [Электронный ресурс] /Brus Schneier // Dr. Dobb's Journal, 1999. Режим доступа: http://www.schneier.com/paper-attacktrees-ddj-ft.html.

2. *Camtepe, S.A.* A Formal Method for Attack Modeling and Detection [Электронный ресурс] /Seyit Ahmet Camtepe, Bulent Yener // TR-06-01, Rensselaer Polytechnic Institute, Computer Science Department. 2006. Режим доступа: http://citeseer.ist.psu.edu/751069.html.

3. *Sheyner, O.* Automated Generation and Analysis of Attack Graphs /Oleg Sheyner, Joshua Haines, Somesh Jha, Richard Lippmann, Jeannette M. Wing // Proceedings of the IEEE Symposium on Security and Privacy. Oakland, CA, USA, 2002. P. 273 – 284.

4. *Jha, S.* Two Formal Analyses of Attack Graphs /S. Jha , O. Sheyner, J. Wing// Proceedings of the 15th IEEE Computer Security Foundations Workshop. Nova Scotia, Canada, June 2002. P. 49-63.

5. *Sheyner, O.* AttackGraph Tool 0.5 [Электронный ресурс]. Режим доступа: http://www.cs.cmu.edu/~odobzins/scenariograph/as_files/AttackGraph-0.5.tar.gz

6. *Von Ohiemb, D.* Formal security analysis with Interacting state machines /David Von Ohiemb, Volkmar Lotz, Dieter Gollmann, Karjoth Günter, Michael Waidner// Lectute Neotes in Computer Science, 2002, № 2502. P. 212-228.

7. Хопкрофт Д. Введение в теорию автоматов, языков и вычислений / Д. Хопкрофт, Р. Мотивани, Д. Ульман // 2-е издание. – М.: Издательский дом «Вильямс», 2002. – 528 с.

8 *Rieke R.* Tool based formal Modelling, Analysis and Visualisation of Enterprise Network Vulnerabilities utilising Attack Graph Exploration [Электронный ресурс]/ *Roland Rieke//* In U.E. Gattiker (Ed.), EICAR 2004 Conference CD-rom: Best Paper Proceedings (ISBN:87-987271-6-8). 31 pages. Copenhagen: EICAR e.V.

9. Poggio, T. A theory of networks for approximation and learning /Poggio, T. Girosi, F.// Technical Report A.I. Memo 1140, Massachusetts Institute of Technology, Artificial Intelligence Laboratory and Center for Biological Information Processing, Whitaker College.

11. *M. H. Stone* (1937). Applications of the Theory of Boolean Rings to General Topology. Transactions of the American Mathematical Society 41 (3), 375–481.

УДК 681.3.06

Е.С. Абрамов, Д.В. Мордвин

ПРИМЕНЕНИЕ МОДЕЛИРОВАНИЯ ОБРАБОТКИ СЕТЕВОГО ТРАФИКА ДЛЯ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ЛВС*

Современные средства противодействия атакам в локальных и глобальных сетях включают в себя межсетевые экраны (МЭ), средства обнаружения вторжений (IDS, intrusion detection system) и средства предотвращения вторжений (IPS, intrusion prevention system). На данном этапе развития данных технологий можно говорить об их взаимной интеграции и возможно окончательном объединении в рамках комплексных решений в будущем. Данные средства действительно позво-

* Работа выполнена при поддержке гранта РФФИ №07-07-00138а.

ляют обнаруживать атаки и противодействовать сетевым атакам, но ни одна из них не может дать гарантий безопасностью в силу собственных ограничений.

В данной статье предлагаются два варианта использования имитационного моделирования локальных сетей для построения системы предотвращения атак, способной преодолеть существующие ограничения.

Рассмотрим существующие средства противодействия атакам и их ограничения. Средства IPS можно считать развитием функциональности средств IDS или даже новым подходом к борьбе с атаками. Если IDS лишь фиксировала атаки и оповещала ответственных лиц об их свершении, то IPS берет на себя задачи принятия решений ограничения части трафика для защиты сети в реальном времени. Тогда можно считать IDS первым шагом в развитии технологии целенаправленной защиты от сетевых атак, а IPS – вторым. Можно в этот список включить и МЭ и считать его нулевым шагом. Тогда схема развития будет выглядеть так: разграничение сетевого трафика (МЭ) – обнаружение вторжений и оповещение (IDS) – блокирование вредоносного трафика (IPS).

Проследим эволюцию ограничений данных систем. Главное ограничение МЭ – невозможность выявить действительно злонамеренный трафик (обнаружить атаку, основываясь на трафике). МЭ способен только на жесткие решения – закрыть порт либо открыть его, заблокировать адрес, либо разрешить его. IDS способна только оповестить администратора о прошедшей атаке, для последующего анализа ситуации. Предотвратить ее возможности не было.

Апогеем развития данных технологий является средство IPS, предотвращающее атаки в реальном времени, но и данная система имеет ограничения, которые наследуются от систем IDS. IDS/IPS можно разделить на два типа:

1. Основанные на обнаружении злоупотреблений.
2. Основанные на обнаружении аномалий.

Вкратце системы первого типа ищут сигнатуры атак в трафике, системы же второго типа ничего не знают об атаках, а обучаются отличать нормальный трафик от аномального. Ограничение систем первого типа – база сигнатур. Ограничение систем второго типа – частота ошибок первого и второго рода (пропуска атак и распознавания аномалии там где ее нет). Следует отметить, что создание систем второго типа – попытка обойти ограничение систем первого типа. Но в настоящий момент ограничения модели обнаружения аномалий (системы второго типа) не позволяют перейти к ее широкомасштабному использованию. Между тем системы первого типа достаточно распространены, постоянно обновляются, но всегда реагируют на новые атаки с запаздыванием. Такое запаздывание вполне достаточно для злоумышленников, среди которых информация о новых уязвимостях распространяется быстрее. Также достаточно быстро создаются программы автоматического использования новой уязвимости.

В данной статье предлагается четвертый этап эволюции средств противодействия атакам – использование моделирования взаимодействующих компонентов ЛВС и проведение вычислительных экспериментов для трафика в режиме реального времени. В основе предлагаемых методов должна лежать реализация модели вычисления сетевых взаимодействий. Другими словами такая система должна быть способна подменить реальную ЛВС. Назовем данную модель виртуальной имитационной сетью (ВИС).

Для описываемых в данной статье методов ВИС должна имитировать защищаемую сеть.

Использование ВИС для предотвращения ограничений систем обнаружения и предотвращения вторжений, основанных на обнаружении злоупотреблений

Данная идея заключается в создании для злоумышленника виртуальной реальности успеха его атаки. Используя возможности средства обнаружения злоупотреблений, мы можем обнаружить известные атаки. Но реакция на обнаруженное вторжение предлагается нестандартная. Вместо отбраковки пакет попадает в ВИС, которая имитирует успех атаки. В дальнейшем трафик злоумышленника на период данной сессии взаимодействия замыкается на ВИС. В ходе сессии ВИС должна выполнить две задачи – одновременно создать для злоумышленника иллюзию успеха вторжения и действий в виртуальной системе и имитировать систему, представляющую минимальный интерес для злоумышленника.

Данный подход основан на предположении, что атаки против конкретной сети чаще всего будут развиваться, начиная с известных приемов, которые могут быть обнаружены существующими средствами IDS. Далее можно предположить, что после общения с описанной выше виртуальной реальностью злоумышленник не станет повторять попытки атак, используя другие методы. Таким образом, можно считать, что данный метод позволит защитить сеть от ранее неизвестных атак путем предотвращения необходимости их применения. Тем самым мы устраняем ограничение лежащих в основе систем обнаружения злоупотреблений.

Использование ВИС для выявления аномалий при обработке трафика путем проведения вычислительных экспериментов в реальном времени

Предлагаемый ниже подход предотвращения вторжений больше похож на существующий. Система на его основе должна действительно останавливать злонамеренный трафик. Такая система должна в реальном времени обнаруживать атаки и делать это до поступления вредоносного трафика в защищаемую сеть. Также описываемый метод предполагает быть эффективнее стандартно используемого для IPS метода обнаружения злоупотреблений на основе сигнатур.

Трафик должен предварительно обрабатываться программной моделью, имитирующей защищаемую сеть (она же ВИС). ВИС должна обладать памятью состояний имитируемых объектов, что позволит системе выявлять распределенные во времени атаки. Каждый объект должен быть предварительно детально изучен и смоделирован таким образом, чтобы обнаруживать аномалии при обработке предназначенного ему трафика. То есть поиск аномалий должен происходить не в содержании сетевых пакетов, а в процессах обработки этих пакетов смоделированным объектом.

Возможности оценки перечня параметров при обработке данных должны быть встроены в качестве агента при проектировании объекта ВИС. Для каждого объекта должны быть выбраны специфичные параметры для оценки агентом. Внедренные агенты должны сигнализировать об обнаруженных аномалиях при обработке пакета данных. Кроме сигнала об обнаружении аномалии агенты должны обладать возможностью сообщать дополнительные сведения о произошедшем событии.

Физически система ВИС должна располагаться на промежуточном шлюзе между защищаемой сетью и внешним соединением. Также предпочтительно соединить описываемую систему с удаленной консолью управления.

В общем виде алгоритм работы ВИС должен выглядеть так:

1. Перехват сетевого пакета, направленного в защищаемую сеть. Загрузка пакета в ВИС.

2. Перенаправление пакета соответствующему моделируемому устройству (хосту или серверу), обработка пакета по стеку TCP/IP.

3. Обработка данных пакета соответствующим конечным приложением.

4. Отправление оригинального пакета в защищаемую сеть. (В алгоритме предлагается использовать отложенное принятие решения.)

5. Опрос встроенных агентов в моделях ВИС, которыми был обработан текущий пакет.

6. Обнаружение агентом аномалии, осуществление реакции заданной пользователем системы (администратором, аналитиком безопасности). Это может быть запись в журналы, отправка сведений об аномалии на локальную или удаленную консоль и ожидание принятие решения по данной сессии взаимодействия ответственным лицом, автоматическая блокировка соединения либо нечто иное, заданное пользователем.

Схема внедрения ВИС для защиты ЛВС представлена на рис. 1.

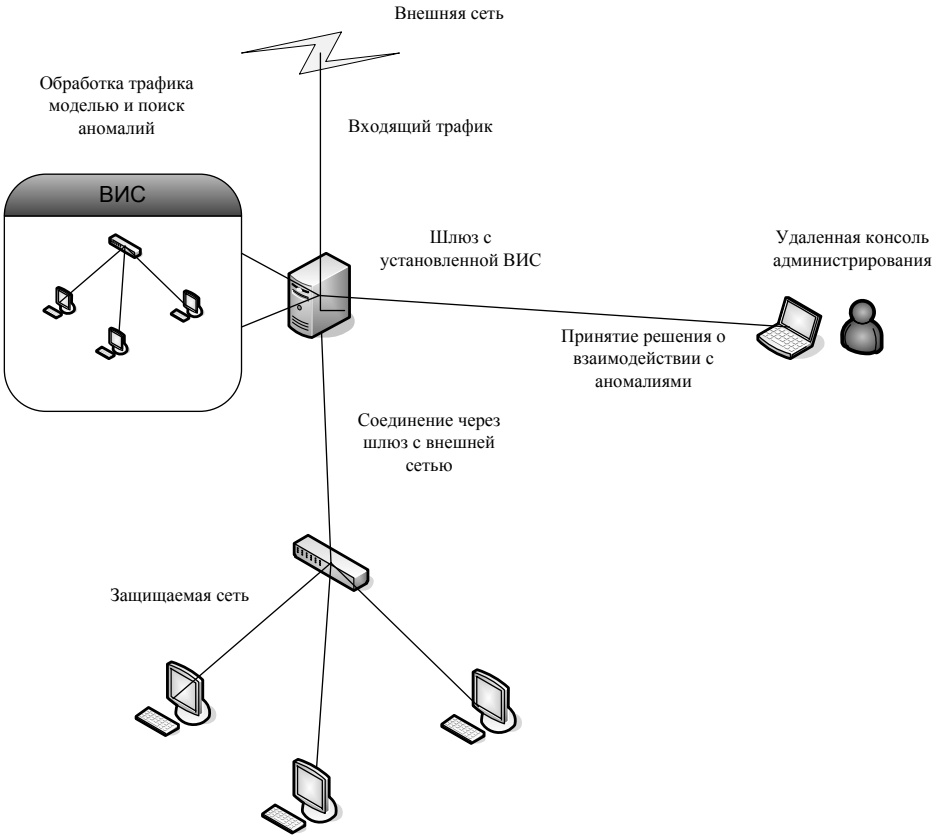

Рис. 1. Схема внедрения ВИС для защиты ЛВС

Описываемый подход изначально предполагается как постоянно обновляемая и расширяемая система. Для каждого реального сетевого объекта (от маршрутизатора до пользовательской программы) может быть смоделирован аналог в ВИС со встроенными агентами оценки аномалий. При добавлении новых компонентов в ВИС ее возможности смогут охватить все большее количество вариантов защи-

щаемых сетей. Такой подход к обнаружению атак не требует длительных и сложных настроек. Администратору достаточно воссоздать в ВИС защищаемую сеть настолько, насколько это позволит текущий набор объектов в ВИС, периодически обновлять объекты. Несложно создать методику автоматической оценки системой защищаемой сети и создания ее аналога в ВИС.

Достоинство данного метода в том, что потенциально возможностей аномалий при обработке трафика гораздо меньше, чем возможное количество сигнатур атак. При этом методы обнаружения аномалий при обработке трафика для различных объектов часто будут достаточно сходны, что еще уменьшает затраты времени на разработку.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Абрамов Е.С.* Разработка комбинированной архитектуры системы обнаружения и выявления сетевых атак. Тезисы докладов на VII Всероссийской НК студентов и аспирантов «Техническая кибернетика, радиоэлектроника и системы управления». – Таганрог: Изд-во ТРТУ, 2004. – 560 с.

2. *Абрамов Е.С., Мордвин Д.В.* Разработка инструментальных средств для моделирования ЛВС // Материалы IX международной научно-практической конференции «Информационная безопасность». – Таганрог: Изд-во ТТИ ЮФУ, 2007.

3. *Абрамов Е.С., Мордвин Д.В.* Создание ложных информационных объектов для противодействия атакам в ЛВС. Материалы X международной научно-практической конференции «Информационная безопасность». – Таганрог: Изд-во ТТИ ЮФУ, 2008.

УДК 004.056

В.А. Нестеренко

ПОСТРОЕНИЕ И ИСПОЛЬЗОВАНИЕ ФУНКЦИИ ПЛОТНОСТИ В ПРОСТРАНСТВЕ ХАРАКТЕРИСТИК ДЛЯ ВЫЯВЛЕНИЯ АНОМАЛЬНЫХ СОБЫТИЙ

Современные методы обнаружения вторжений, основанные на выявлении аномальных событий, в основном построены по следующему принципу: вначале создаётся модель нормального поведения, характеризующая состояние системы в отсутствие нарушений, а затем выявляются отклонения наблюдаемых данных от нормального поведения [1]. Одним из методов построения модели нормального поведения системы является кластеризация данных [2]. В основе этого метода лежит допущение о том, что в пространстве числовых характеристик событий множество данных кластеризуется – собирается в отдельные группы. При подходящем выборе набора характеристик нормальные и аномальные события различимы – они группируются в разных кластерах. Кроме того, делается предположение о том, что число нормальных событий заметно превышает число аномальных событий, т.е. нормальные события формируют большие кластеры.

Для кластеризации данных применяются различные методы [3]: разделяющие методы, решёточные методы, методы основанные на плотности. В предлагаемой работе рассматривается метод кластеризации использующий оценку плотности в пространстве характеристик событий. Основная идея этого метода заключается в том, что некоторая область пространства принадлежит кластеру в том случае, если плотность событий в этой области превышает заданную пороговую величину. Подобные методы хорошо подходят для фильтрации выбросов и для создания кластеров произвольной формы.