УДК 681.3.053:681.32:007.5

МОДЕЛИ ДЕЙСТВИЙ ХАКЕРОВ-ЗЛОУМЫШЛЕННИКОВ ПРИ РЕАЛИЗАЦИИ РАСПРЕДЕЛЕННЫХ МНОГОШАГОВЫХ АТАК*

И.В. Котенко[1], М.В. Степашкин[2]

В работе рассмотрен основанный на экспертных знаниях подход к моделированию действий хакеров-злоумышленников. Данный подход базируется на использовании комплекса моделей, в частности, моделей реализации компьютерных атак, моделей нарушителя и моделей формирования общего графа атак, задающего все возможные способы компрометации компьютерной сети. Представлены аспекты построения указанных моделей, их реализация и пример применения для оценки защищенности компьютерных сетей.

Введение

Актуальным направлением исследований в области искусственного интеллекта является моделирование действий активных агентов в сложных динамических средах. Одним из важных примеров таких задач является моделирование действий хакеров-злоумышленников в процессе реализации ими распределенных многошаговых атак на компьютерные сети (КС). Используя комбинации имеющихся уязвимостей и недостатков в конфигурации сети и применяемой политике безопасности, нарушители (как внешние, так и внутренние), в зависимости от своих целей, могут реализовать разнообразные стратегии нападения. Эти стратегии могут быть направлены на различные критические ресурсы сети, и включать разнообразные цепочки атакующих действий.

Моделирование действий хакеров-злоумышленников может помочь, например, найти ответы на следующие вопросы: (1) каковы мотивы, цели и стратегии злоумышленников; (2) как зависят результаты и способы

* Работа выполнена при финансовой поддержке РФФИ (проект №04-01-00167), программы фундаментальных исследований ОИТВС РАН (контракт №3.2/03) и при частичной финансовой поддержке, осуществляемой в рамках проекта Евросоюза POSITIF (контракт IST-2002-002314)

[1] *199178, С.-Петербург, 14 линия, 39, СПИИРАН, ivkote@comsec.spb.ru*

[2] *199178, С.-Петербург, 14 линия, 39, СПИИРАН, stepashkin@comsec.spb.ru*

действий нарушителей от их квалификации и уровня знаний; (3) насколько адекватны реализованные в компьютерной сети механизмы безопасности существующим рискам; (4) имеются ли в текущей конфигурации используемого аппаратного и программного обеспечения ошибки, позволяющие потенциальным нарушителям обойти механизмы разграничения доступа; (5) содержит ли используемое в сети программное обеспечение уязвимости, которые могут быть использованы для взлома защиты; (6) как оценить уровень защищенности компьютерной сети и как определить является ли он достаточным в данной среде функционирования.

В настоящее время существует много работ, раскрывающих различные подходы к моделированию атак и анализу защищенности на этапе проектирования: метод анализа изменения состояний [Chung et al., 1995], причинно-следственная модель атак [Cohen, 1999], описательные модели сети и злоумышленников [Yuill et al., 2000], структурированное описание на базе деревьев [Dawkins et al., 2002], использование и создание графов атак для анализа уязвимостей [Iglun et al., 1995], объектно-ориентированное дискретное событийное моделирование [Chi et al., 2001] и другие. В работе рассматривается *подход к моделированию действий хакеров-злоумышленников, учитывающий разнообразие знаний, целей и местоположения нарушителя, конфигураций компьютерной сети и правил реализуемой политики безопасности*. Он базируется на использовании комплекса моделей, основанных на экспертных знаниях, в том числе моделей атак, нарушителей и формирования графа атак, задающего возможные способы компрометации компьютерной сети [Kotenko et al., 2005].

Работа организована следующим образом. В *первом разделе* описывается модель компьютерных атак, на основе которой имитируются действия нарушителя. Во *втором разделе* кратко представлена используемая модель нарушителя. *Третий раздел* содержит основные идеи, положенные в основу формирования общего графа атак. В *четвертом разделе* рассмотрено практическое применение предложенных моделей на примере задачи анализа защищенности. В *заключении* формулируются результаты работы и направления будущих исследований.

1. Интегрированная модель компьютерных атак

Модель компьютерных атак служит для описания возможных действий нарушителя и формирования сценариев реализации этих действий. *Интегрированная модель атак* $M_{KA} = \left\langle M_{KA}^{KY}, M_{KA}^{CY}, M_{KA}^{HY} \right\rangle$ имеет вид иерархической структуры, состоящей из моделей нескольких уровней

(рис. 1) [Котенко и др., 2005]. Связи на рис.1 могут отражать различные отношения между объектами модели атак: “целое — часть”, “понятие — класс понятия”, “операция — этап реализации”, “тип объекта — экземпляр объекта” и “предыдущий — последующий элемент в цепочке действий”. Модель комплексного уровня $M_{KA}^{KУ}$ определяет множество высокоуровневых целей, обеспечивая согласование нескольких сценариев, которые могут быть реализованы группой нарушителей. Модель сценарного уровня $M_{KA}^{CУ}$ определяет только одну высокоуровневую цель и уточняет подцели атаки. Модель нижнего уровня $M_{KA}^{KУ}$ в иерархии описывает низкоуровневые действия нарушителя, например, по запуску программ реализации атак (эксплоитов), выполнению команд операционной системы (ОС) и т.п.

Модель комплексного уровня служит для параметризации различных высокоуровневых аспектов моделирования действий хакеров-злоумышленников: $M_{KA}^{KУ} = \langle M_A, G, T_G, P_{ML} \rangle$, где M_A — модель нарушителя; G — граф, представляющий этапы сценариев и нижележащие уровни модели компьютерных атак без низкоуровневых атакующих действий; T_G — высокоуровневая цель, описывающая процесс моделирования (например, проимитировать все возможные угрозы безопасности, исследовать реализацию угрозы нарушения доступности и др.); P_{ML} — уровень моделирования (уровень идентификаторов

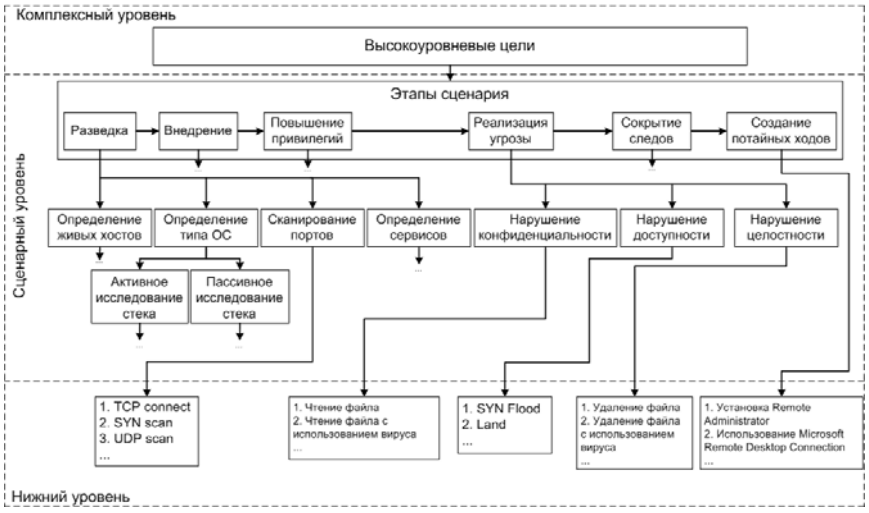

Рис. 1. Представление модели компьютерных атак

атакующих действий или низкоуровневого представления в виде последовательности сетевых пакетов).

Высокоуровневая цель T_G, описывающая процесс моделирования атак, состоит из двух компонент: (1) множество объектов O, которые подвергаются анализу (пустое множество, отдельный хост, множество хостов) и (2) множество высокоуровневых целей $T_{GS} \subset T_{HL}$, $T_{HL} = \{\text{Доступность}, \text{Конфиденциальность}, \text{Целостность}\}$, определяющих, какие составляющие компьютерной безопасности необходимо проанализировать: $T_G = \langle O, T_{GS} \rangle$.

Модель атак сценарного уровня служит для генерации последовательности атакующих действий (сценария) с учетом цели, которая должна быть достигнута с использованием данного сценария, различных характеристик, описывающих модель злоумышленника и т.п. Сценарий представляет собой последовательность атакующих действий: $S = \{a_i\}_{i=1}^{N_S}$, где N_S — длина сценария. Данная модель представляется в следующем виде: $M_{KA}^{CV} = \langle G_A, T_S, P_L, M_{SG} \rangle$, где G_A — граф атакующих действий, на базе которого строится сценарий; T_S — цель, которая должна быть достигнута выполнением сценария; P_L — местоположение злоумышленника, задаваемое представлением хоста модели анализируемой компьютерной сети; M_{SG} — метод генерации сценария.

Граф атакующих действий G_A содержит этапы сценариев, все нижележащие уровни, представленные в общей модели компьютерных атак, и низкоуровневые атакующие действия с учетом уровня знаний нарушителя. Цель, достигаемая выполнением сценария, $T_S = \langle o, T_A \rangle$, где o — атакуемый объект, задаваемый представлением хоста модели анализируемой компьютерной сети; T_A — высокоуровневая цель атаки, которая является элементом множества высокоуровневых целей, отвечающих за нарушение основных составляющих компьютерной безопасности: $T_A \in T_{HL}$.

В данной модели компьютерных атак используются три метода генерации сценария M_{SG}: (1) прямой вывод; (2) обратный вывод и (3) комбинированный. При реализации метода, использующего прямой вывод в сценарий S попадают все доступные низкоуровневые атакующие действия для каждого этапа сценария, начиная с первого. Метод обратного вывода подразумевает создание оптимизированного сценария (при этом генерация сценария начинается с последнего действия в получаемой цепочке действий). Комбинированный метод позволяет сочетать для

формирования различных этапов сценария как прямой вывод, так и обратный. Таким образом, сценарий формируется методом M_{SG} на основе графа атакующих действий G_A, информации о местоположении злоумышленника P_L и цели, которая должна достигаться данным сценарием: $S = \{a_i\}_{i=1}^{N_S} = M_{SG}(G_A, T_S, P_L)$.

Модель атак нижнего уровня представляет собой множество атакующих действий A: $M_{KA}^{HY} = \langle A \rangle$, где $A = \{a_i\}_{i=1}^{N_A}$, где N_A — количество всех атакующих действий. Каждое атакующее действие записывается в следующем виде: $a_i = \langle c_i, e_i, r_i \rangle \; \forall i \in [1, N_A]$, где c_i — условие выполнимости атакующего действия; e_i — представление воздействия на атакуемый объект; r_i — результат атакующего действия.

Формальное представление условия выполнимости атакующего действия c_i и его результата r_i описывается в виде шаблона объекта *модели анализируемой компьютерной сети*, которая содержит перечень устройств (например, D — сетевые устройства, H — множество хостов, Sv — множество сетевых концентраторов, $D \equiv H \cup S$) и их основные характеристики (используемая ОС, список сетевых сервисов, параметры настройки протокола TCP/IP и т.п.). Например, на естественном языке шаблон может быть выражен следующим образом: “хост с открытым портом TCP 80”.

2. Модель нарушителя

При формировании сценариев реализации атакующих действий необходимо учитывать множество параметров, характеризующих нарушителя (его уровень знаний и умений, множество доступных программных и аппаратных средств по реализации атак, первоначальное положение и т.п.), т.е. необходимо построить модель нарушителя. Модель нарушителя тесно связана с моделью компьютерных атак. Взаимосвязь данных двух моделей состоит в следующем: в модели компьютерных атак содержится максимально полное описание возможных способов компрометации объекта защиты, а модель нарушителя конкретизирует кто, какими средствами и с использованием каких знаний может реализовать данные угрозы и нанести ущерб объекту защиты.

Нарушитель характеризуется следующими параметрами: (1) местоположение (по данному параметру нарушителей можно условно разделить на две группы: внутренние и внешние); (2) уровень знаний и умений (например, нарушитель обладает глубокими знаниями ОС семейства Windows); (3) первичные знания об атакуемой компьютерной

сети (например, нарушителю известна топология КС, но не известны используемые сетевые сервисы); (4) используемый метод формирования сценария.

Модель нарушителя представляется следующим образом: $M_A = \langle P_L, P_{KL}, K_N, m_{SG} \rangle$, где P_L — местоположение нарушителя; P_{KL} — уровень знаний и умений; K_N — первичные знания об атакуемой компьютерной сети; m_{SG} — используемый метод формирования сценария.

Местоположение нарушителя задается представлением хоста модели анализируемой компьютерной сети.

Выделяется три уровня знаний и умений нарушителя: $P_{KL} \in \{1,2,3\}$, где 1 — низкий уровень знаний и умений, 2 — средний и 3 — высокий. Каждый вышележащий уровень включает возможности (знания и умения) всех нижележащих уровней. В реализованной модели различным уровням знаний соответствуют различные структуры знаний об используемых уязвимостях и эксплоитах.

Первичные знания об атакуемой компьютерной сети K_N описываются с использованием модели анализируемой компьютерной сети (в виде множества известных нарушителю устройств, их характеристик и правил функционирования, описываемых политикой безопасности).

3. Модель формирования общего графа атак

Для построения графа атакующих действий G_A, используемого на сценарном уровне модели компьютерных атак, необходимо дополнить граф G комплексного уровня низкоуровневыми действиями, информацию о которых можно получить, используя открытые базы уязвимостей [NVD, 2006; OSVDB, 2006], и учесть при этом уровень знаний нарушителя.

Обозначим множество всех уязвимостей $VDB = \{vul_i\}_{i=1}^{N_{VDB}}$, где N_{VDB} — общее количество уязвимостей. Для каждой уязвимости vul_i определяется необходимый уровень знаний и умений нарушителя vul_i^{KL}, способного ее использовать. Затем для каждой группы нарушителей определяется множество используемых ею уязвимостей: $VDB_{KL} = \{vul_i \times P_{KL}\}_{i=1}^{N_{VDB}}$, где $vul_i \times P_{KL} = \begin{cases} vul_i, vul_i^{KL} \le P_{KL} \\ 0, vul_i^{KL} > P_{KL} \end{cases}$. Тогда вершины графа G_A: $V_{GA} = V_G \cup VDB_{KL}$ при $\forall i \in \left[1..\left|VDB_{KL}\right|\right] \exists k : v_k \in V_G,\ link(v_k, vul_i) \neq \varnothing$.

Общий граф атак описывает все возможные варианты реализации атакующих действий нарушителем с учетом его первоначального

положения, уровня знаний и умений, первоначальной конфигурации компьютерной сети и реализуемой в ней политики безопасности. На основе общего графа атак производится анализ защищенности компьютерной сети, определение «узких» мест, формирование рекомендаций по устранению обнаруженных уязвимостей с учетом их уровня критичности.

Для формирования общего графа атак используется алгоритм, основанный на реализации следующей последовательности действий:

(1) реализация действий по перемещению нарушителя с одного хоста на другой,

(2) реализация разведывательных действий по определению живых хостов,

(3) реализация сценариев (множества действий) разведки для каждого обнаруженного хоста и

(4) реализация атакующих действий, использующих уязвимости программного и аппаратного обеспечения и общих действий пользователя.

4. Практическое применение разработанных моделей

Одной из областей применения моделирования действий нарушителя является анализ защищенности. В настоящее время разработана перспективная система анализа защищенности (САЗ), в основу которой положены рассмотренные модели. Пример графического интерфейса САЗ приведен на рис. 2. В основном окне интерфейса представлен пример общего графа атак, полученного в результате моделирования действий нарушителей.

Основными функциональными возможностями предлагаемой САЗ являются: (1) актуализация информации об известных уязвимостях в программном и аппаратном обеспечении из внешних баз данных уязвимостей; (2) обновление базы данных обычных действий рядовых пользователей, которые могут также как и действия, использующие уязвимости, нарушать информационную безопасность; (3) загрузка спецификаций анализируемой компьютерной сети и реализуемой в ней политики безопасности, заданных на специализированных языках; (4) задание пользователем модели нарушителя (множества параметров, отражающих уровень его знаний, первоначальное положение и т.п.); (5) задание пользователем требований к уровню защищенности сети; (6) моделирование действий нарушителя и построение общего графа атак; (7) анализ общего графа атак и расчет множества метрик, отражающих с разной степенью детализации защищенность анализируемой компьютерной сети; (8) формирование отчетов, содержащих перечень обнаруженных уязвимостей, “узких мест”, рекомендации по повышению общего уровня защищенности анализируемой сети.

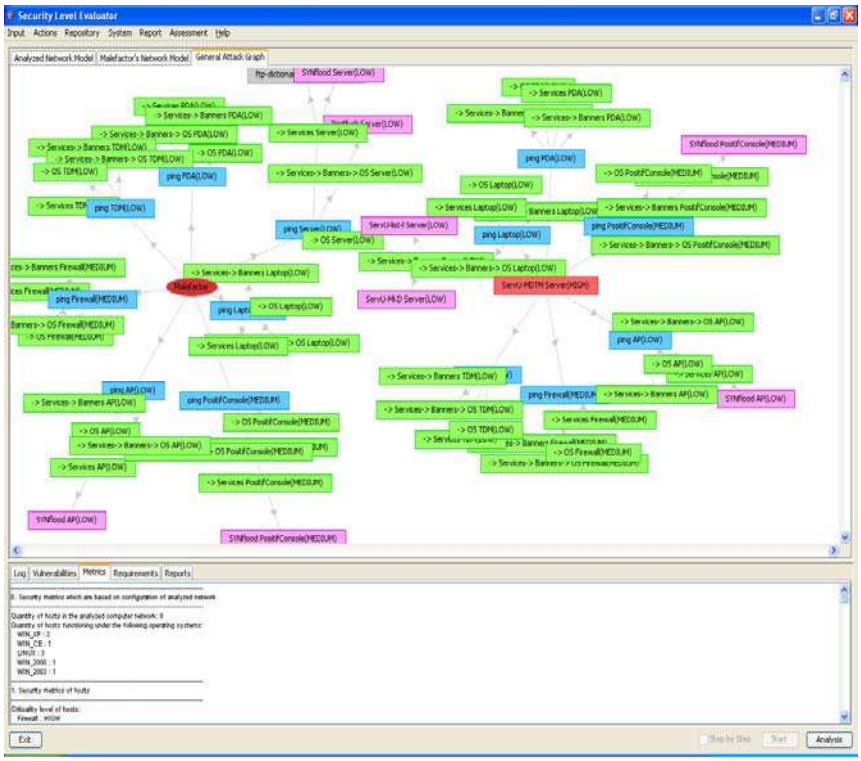

Рис. 2. Графический интерфейс пользователя системы анализа защищенности

Данная система анализа защищенности может использоваться как на этапе проектирования компьютерной сети, так и на этапе ее эксплуатации [Kotenko et al., 2005]. В первом случае входными данными для САЗ являются спецификации сети и реализуемой в ней политики безопасности, создаваемые проектировщиком. Во втором случае спецификации формируются на основе данных, получаемых с помощью программных агентов, расположенных на различных хостах компьютерной сети.

4. Заключение

В работе рассмотрен подход к моделированию действий хакеров-злоумышленников, учитывающий их первоначальное положение, уровень знаний и умений, разнообразие целей, конфигурации компьютерной сети и реализуемые в ней политики безопасности.

Данный подход был реализован в разработанной системе анализа защищенности, проведены многочисленные эксперименты по анализу защищенности компьютерных сетей с различной конфигурацией и политикой безопасности.

Предложенный подход и реализованная система могут быть использованы для разработки новых методов защиты, оценки уровня защищенности компьютерных сетей на различных этапах их жизненного цикла, разработки принципиально новых средств защиты информации.

Направлениями дальнейших исследований являются совершенствование предложенных моделей, используемых для моделирования действий нарушителя, развитие функциональности разработанной системы анализа защищенности на этапах их проектирования и эксплуатации, базирующейся на данных моделях.

Список литературы

[Котенко и др., 2005] Котенко И. В., Степашкин М. В., Богданов В. С. Архитектуры и модели компонентов активного анализа защищенности на основе имитации действий злоумышленников // Проблемы информационной безопасности. Компьютерные системы. № 4. — СПб., 2005.

[Chi et al., 2001] Chi S.-D., Park J. S., Jung K.-C., Lee J.-S. Network security modeling and cyber attack simulation methodology // Lecture Notes in Computer Science. Springer-Verlag, 2001. Vol. 2119.

[Chung et al., 1995] Chung M, Mukherjee B., Olsson R. A., Puketza N. Simulating Concurrent Intrusions for Testing Intrusion Detection Systems // Proceedings of the 18th NISSC. 1995.

[Cohen, 1999] Cohen F. Simulating Cyber Attacks, Defenses, and Consequences. IEEE Symposium on Security and Privacy, Berkeley, CA. 1999.

[Dawkins et al., 2002] Dawkins J., Campbell C., Hale J. Modeling network attacks: Extending the attack tree paradigm // Workshop on Statistical and Machine Learning Techniques in Computer Intrusion Detection, Johns Hopkins University. 2002.

[Iglun et al., 1995] Iglun K., Kemmerer R. A., Porras P. A. State Transition Analysis: A Rule-Based Intrusion Detection System // IEEE Transactions on Software Engineering, V.21, No. 3. 1995.

[Kotenko et al., 2005] Kotenko I. V., Stepashkin M. V. Analyzing Vulnerabilities and Measuring Security Level at Design and Exploitation Stages of Computer Network Life Cycle // Lecture Notes in Computer Science. Springer-Verlag, 2005. Vol. 3685.

[NVD, 2006] NVD: National Vulnerability Database. http://nvd.nist.gov/. 2006.

[OSVDB, 2006] OSVDB: The Open Source Vulnerability Database. http://www.osvdb.org/ . 2006.

[Yuill et al., 2000] Yuill J., Wu F., Settle J., Gong F. Intrusion-detection for incident-response, using a military battlefield-intelligence process // Computer Networks, No.34. 2000.