УДК 681.3.053:681.32:007.5

МОДЕЛИ И МЕТОДИКА ИНТЕЛЛЕКТУАЛЬНОЙ ОЦЕНКИ УРОВНЯ ЗАЩИЩЕННОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ*

И.В. Котенко[1], М.В. Степашкин[2], В.С. Богданов[3]

В работе представлен подход к интеллектуальной оценке уровня защищенности компьютерных сетей. Подход базируется на применении комплекса моделей, основанных на экспертных знаниях. В частности, используются модели компьютерных атак и нарушителя, модели построения общего графа атак, модели компьютерной сети и оценки уровня защищенности. Особое внимание в работе уделено модели построения общего графа атак, который описывает всевозможные варианты реализации нарушителем атакующих действий. Представлена также методика экспресс оценки уровня защищенности компьютерной сети.

Введение

Возросшая сложность компьютерных сетей и механизмов защиты, увеличение количества уязвимостей и потенциальных ошибок в их использовании, а также возможностей по реализации атак обуславливают необходимость разработки мощных автоматизированных интеллектуальных систем анализа защищенности компьютерных сетей [McNab, 2004]. Эти системы призваны выполнять задачи по обнаружению и исправлению ошибок в конфигурации сети, выявлению возможных трасс атакующих действий различных категорий нарушителей (по реализации различных угроз безопасности), определению критичных сетевых ресурсов и выбору адекватной угрозам политики безопасности,

* 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, Санкт-Петербург, 14 линия, д. 39, СПИИРАН, ivkote@comsec.spb.ru*

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

[3] *199178, Санкт-Петербург, 14 линия, д. 39, СПИИРАН, bogdanov@comsec.spb.ru*

которая задействует наиболее подходящие в заданных условиях защитные механизмы.

Настоящая работа направлена на создание моделей, которые обеспечат базис для создания интеллектуальных систем анализа защищенности компьютерных сетей. В первом разделе кратко описаны модели компьютерных атак и нарушителя. Второй раздел посвящен модели формирования общего графа атак. Третий раздел содержит описание модели анализируемой компьютерной сети, а также модели и методики оценки уровня защищенности. В заключении формулируются результаты работы и направления дальнейших исследований.

1. Модели компьютерных атак и нарушителя

1.1. Модель компьютерных атак используется для описания возможных действий нарушителя и формирования сценариев реализации этих действий. Данная модель имеет вид иерархической структуры, состоящей из нескольких уровней [Kotenko et al, 2005].

Верхними уровнями являются комплексный и сценарный уровни. Комплексный уровень определяет множество высокоуровневых целей процесса анализа защищенности (анализ на нарушение основных аспектов компьютерной безопасности: целостности, конфиденциальности, доступности) и множество анализируемых (атакуемых) объектов. На комплексном уровне может быть обеспечено согласование нескольких сценариев, которые реализуются группой нарушителей. Сценарный уровень учитывает модель нарушителя, определяет конкретный атакуемый объект (один хост) и цель атаки (например, «определение ОС хоста», «реализация атаки отказа в обслуживании» и т.п.).

Сценарный уровень содержит этапы сценария, множество которых состоит из следующих элементов: (1) разведка, (2) внедрение (первоначальный доступ к хосту), (3) повышение привилегий; (4) реализация угрозы; (5) сокрытие следов; (6) создание потайных ходов. Нижележащие элементы сценарного уровня служат для детализации цели, достигаемой реализацией сценария.

Нижний уровень в иерархии концептуальной модели компьютерных атак описывает низкоуровневые атакующие действия нарушителя и эксплоиты.

1.2. 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.

Модель нарушителя позволяет учесть следующие его параметры:

(1) первоначальное положение (внутренние и внешние нарушители);

(2) уровень знаний и умений, определяющий возможности нарушителя по реализации атакующих действий (задается перечнем известных нарушителю уязвимостей, средств реализации атаки и т.п.);

(3) первичные знания об атакуемой компьютерной сети (в виде перечня хостов, пользователей и т.п.);

(4) используемый метод генерации сценария (используется ли оптимизация сценария для достижения заданной цели).

2. Модель формирования общего графа атак

Модель формирования общего графа атак служит для построения графа, описывающего всевозможные 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.

2.1. Объекты общего графа атак. Все объекты графа атак можно подразделить на базовые объекты и составные. Вершины графа задаются с использованием базовых объектов. Для формирования различных последовательностей действий нарушителя базовые объекты связываются на графе атак с помощью дуг. Таким образом формируются составные объекты графа. К базовым объектам общего графа атак относятся объекты, принадлежащие к типам «хост» и «атакующее действие». Множество объектов «хосты» включает все обнаруженные нарушителем и атакуемые им сетевые компьютеры (хосты). Множество объектов «атакующие действия» состоит из всех различимых элементарных действий нарушителя.

Атакующие действия разделены на следующие классы: (1) действия по получению информации о сети (хосте), т.е. разведывательные действия; (2) подготовительные действия (в рамках уже имеющихся у нарушителя полномочий), служащие для создания условий реализации атакующих действий последующих классов; (3) действия, направленные на нарушение конфиденциальности; (4) действия, направленные на нарушение целостности; (5) действия, направленные на нарушение доступности; (6) действия, приводящие к получению нарушителем прав

локального пользователя; (7) действия, приводящие к получению нарушителем прав администратора.

Все атакующие действия можно разделить также на две группы:

(1) действия, использующие различные уязвимости программного и аппаратного обеспечения, например, «NTP_LINUX_ROOT» (использует уязвимость в сервисе NTP ОС семейства Linux и позволяет нарушителю получить права администратора на атакуемом хосте);

(2) обычные действия легитимного пользователя системы (в том числе действия по использованию утилит получения информации о хосте или сети), такие как «удаление файла», «остановка сервиса ОС» и т.п.

К составным объектам отнесем объекты типов «трасса», «угроза» и «граф». Трасса атаки — это совокупность связанных вершин общего графа атак (хостов и атакующих действий), первая из которых представляет хост, соответствующий первоначальному положению нарушителя, а последняя не имеет исходящих дуг. Под угрозой будем понимать множество различных трасс атак, имеющих одинаковые начальную и конечную вершины.

Разделение атакующих действий по заданным выше классам, позволяет классифицировать угрозы следующим образом:

(1) основные угрозы — угрозы нарушения конфиденциальности, угрозы нарушения целостности, угрозы нарушения доступности;

(2) дополнительные угрозы — угрозы получения информации о сети (хосте), угрозы получения нарушителем прав локального пользователя или прав администратора.

В общем случае, при успешной реализации нарушителем разведывательных действий, не происходит нарушения конфиденциальности, целостности и доступности информационных ресурсов. Однако, возможно нарушение конфиденциальности, например, в том случае, если политикой безопасности установлено, что информация о топологии внутренней сети является закрытой. При успешном получении нарушителем прав локального пользователя, возможности выполнения действий, направленных на нарушение конфиденциальности, целостности и доступности, или на получение прав администратора увеличиваются, так, например, он может нарушить конфиденциальность, целостность и доступность некоторой совокупности объектов хоста, имея только права пользователя. При успешном получении прав администратора на хосте нарушитель может полностью нарушить конфиденциальность, целостность, доступность всех объектов данного хоста.

В направлении роста степени сложности все объекты графа атак можно упорядочить следующим образом (стрелка показывает

направление увеличения вложенности объектов): хосты, атакующие действия → трассы атак → угрозы → общий граф атак.

2.2. Обобщенный алгоритм формирования общего графа атак основан на реализации следующей последовательности действий:

(1) действия по перемещению нарушителя с одного хоста на другой;

(2) разведывательные действия по определению живых хостов;

(3) действия разведки для каждого обнаруженного хоста;

(4) атакующие действия, использующие уязвимости программного и аппаратного обеспечения и общих действий пользователя.

Вначале фиксируется первоначальное положение нарушителя. Перемещение нарушителя с текущего хоста на атакуемый хост осуществляется при получении нарушителем на атакуемом хосте прав локального пользователя или администратора в следующих случаях: (1) если существует возможность реализации атакующих действий, использующих уязвимости программного и аппаратного обеспечения и требующих у нарушителя наличия прав локального пользователя на атакуемом хосте; (2) если переход на атакуемый хост открывает нарушителю доступ к другому сегменту сети; (3) если переход на атакуемый хост позволяет нарушителю использовать отношения доверия.

Примером разведывательного действия по определению живых хостов является действие, эмулирующее работу утилиты «ping». Примерами разведывательных действий, на основе которых формируется множество сценариев разведки, являются следующие действия: (1) «nmap OS» – реализация данного низкоуровневого действия позволяет нарушителю узнать тип и (возможно) точную версию операционной системы; (2) «nmap services» – реализация данного низкоуровневого действия позволяет нарушителю получить список открытых на хосте портов; (3) «banners» – реализация данного низкоуровневого действия позволяет нарушителю получить названия и версии функционирующих на хосте сетевых сервисов путем анализа баннеров. Таким образом, при формировании общего графа атак сценарии атак будут содержать комбинации данных низкоуровневых действий. Так как некоторые комбинации будут приводить к одинаковому результату, выделим следующие сценарии разведывательных действий нарушителя, приводящие к различным результатам: (1) «nmap OS»; (2) «nmap services»; (3) «nmap services» → «banners»; (4) «nmap services» → «banners» → «nmap OS». Из вышеперечисленных сценариев формируется множество сценариев разведки.

После реализации каждого сценария из множества сценариев разведки производится проверка условий выполнения атакующих действий, использующих уязвимости программного и аппаратного обеспечения и

общих действий пользователя. При успешной реализации атакующих действий данной группы, приводящих к получению нарушителем прав локального пользователя или администратора на атакованном хосте, осуществляется проверка необходимости перехода нарушителя на данный хост. В случае реализации перехода, вышеописанная последовательность действий повторяется для нового положения нарушителя.

3. Модели компьютерной сети и оценки уровня защищенности. Методика экспресс оценки общего уровня защищенности

3.1. Модель анализируемой компьютерной сети служит для представления используемого в сети программного и аппаратного обеспечения, распознавания действий нарушителя и определения реакции сети на реализуемые нарушителем атакующие действия. Для спецификации аппаратного и программного обеспечения предлагается использовать специализированный язык System Description Language (SDL). SDL представляется в формате Common Information Model (CIM) [CIM, 2006]. CIM — это способ управления автоматизированными системами, приложениями, сетями и сервисами, разработанный Distributed Management Task Force (DMTF) и использующий основные объектно-ориентированные технологии структурирования и концептуализации. SDL описывает компьютерную сеть на уровне ее топологии и сетевых сервисов. Сетевая топология описывается классами PhysicalElement, PhysicalLink, и ассоциации ElementsLinked. Сетевые сервисы описываются классами ComputerSystem, Service, ProtocolEndpoint, ServiceAccessPoint, ServiceAvailableToElement, ProvidesEndpoint, HostedAccessPoint, BindsTo. Распознавание действий нарушителя необходимо для преобразования низкоуровневого представления атакующих действий (последовательности сетевых пакетов или команд ОС) в высокоуровневые идентификаторы атак. В основу функционирования данного механизма положен сигнатурный метод — поступающая на вход модели компьютерной сети последовательность сетевых пакетов или команд ОС сравнивается с заранее определенными сигнатурами и в случае обнаружения сходства определяется высокоуровневый идентификатор атаки. В ответ на реализацию нарушителем атакующих действий производится обновление модели анализируемой сети (с использованием представления атакующих действий из модели компьютерных атак), например, остановка сетевого сервиса, удаление файла и т.п.

3.2. Модель оценки уровня защищенности охватывает систему различных метрик безопасности и правил (формул), используемых для их расчета. Множество всех метрик безопасности строится на основе сформированного общего графа атак. Метрики безопасности могут

характеризовать защищенность как базовых, так и составных объектов графа атак. Метрики безопасности можно классифицировать по следующим признакам [Котенко и др., 2006]: (1) по разделению объектов общего графа атак на базовые и составные; (2) в соответствии с порядком вычислений; (3) в соответствии с тем, используются ли метрики для определения общего уровня защищенности анализируемой компьютерной сети. Примерами метрик безопасности являются: (1) критичность хоста; (2) размер ущерба при реализации угрозы; (3) количество трасс атак на графе и т.д.

3.3. Методика экспресс оценки общего уровня защищенности компьютерной сети основана на методике FRAP [FRAP, 2006] и состоит из следующих этапов: (1) определение уровня критичности хостов ($Criticality(h)$) по трехуровневой шкале (High, Medium, Low); (2) определение критичности атакующих действий ($Severity(a)$) на основе алгоритма CVSS [CVSS, 2006] получения обобщенной оценки критичности атакующего действия; (3) определение размера ущерба ($Mortality(a,h)$), вызванного успешной реализацией атакующего действия, зависящего от уровней критичности действия и атакуемого хоста; (4) определение размера ущерба для всех угроз ($Mortality(T) = Mortality(a_T, h_T)$, где a_T — последнее атакующее действие угрозы, направленное на хост h_T); (5) определение метрик сложности в доступе для всех атакующих действий ($AccessComplexity(a)$), для всех трасс ($AccessComplexity(S)$) с учетом значений данного показателя для всех действий, составляющих трассу, и всех угроз ($AccessComplexity(T)$) с учетом значений данного показателя для всех трасс, составляющих угрозу; (6) определение степени возможности реализации угрозы ($Realization(T)$) на основе показателя сложности в доступе; (7) определение общего уровня защищенности компьютерной сети ($SecurityLevel$) на базе полученных оценок степени реализации угрозы и размера ущерба, вызванного ее успешной реализацией.

Заключение

В работе предложен подход к интеллектуальной оценке уровня защищенности компьютерных сетей на базе построения общего графа атак, обладающий следующими особенностями: (1) использование для анализа защищенности комплекса различных моделей, построенных на экспертных знаниях, в том числе моделей нарушителя, моделей

компьютерных атак, формирования общего графа атак, расчета метрик защищенности и определения общего уровня защищенности; (2) учет разнообразия местоположения, целей и уровня знаний нарушителя; (3) использование при построении общего графа атак не только параметров конфигурации компьютерной сети, но и правил реализуемой политики безопасности; (4) учет как собственно атакующих действий (по использованию уязвимостей), так и разрешенных действий пользователя и действий по разведке; (5) возможность исследования различных угроз безопасности для различных ресурсов сети; (6) возможность определения «узких мест» (хостов, ответственных за большее количество трасс атак и уязвимостей, имеющих наиболее высокую возможность компрометации); (7) возможность задания запросов к системе вида «что если», например, какова будет защищенность при изменении определенного параметра конфигурации сети, правила политики безопасности; (8) применение для построения графа атак актуализированных баз данных об уязвимостях (например, OSVDB [OSVDB, 2006]); (9) использование для расчета части первичных метрик защищенности подхода CVSS [CVSS, 2006]; (10) применение для вычисления метрик защищенности качественных методик анализа риска (в частности, модифицированной методики оценки серьезности сетевой атаки SANS/GIAC и методики FRAP [FRAP, 2006]).

Для практической оценки предложенного подхода разработан программный прототип интеллектуальной системы анализа защищенности [Котенко и др., 2006].

Направлениями дальнейших исследования являются развитие предложенных моделей и программного прототипа интеллектуальной системы анализа защищенности компьютерных сетей, оценка эффективности предложенного подхода.

Список литературы

[Котенко и др., 2006] Котенко И. В., Степашкин М. В. Метрики безопасности для оценки уровня защищенности компьютерных сетей на основе построения графов атак // Защита информации. INSIDE. №3, 2006.

[CIM, 2006] CIM. Common Infromation Model [Электронный ресурс] // <http://www.dmtf.org/standards/cim> (по состоянию на 01.01.2006).

[CVSS, 2006] CVSS. Common Vulnerability Scoring System [Электронный ресурс] // <http://www.first.org/cvss/> (по состоянию на 17.03.06).

[FRAP, 2006] FRAP. Facilitated Risk Analysis Process [Электронный ресурс] // <http://www.peltierassociates.com/> (по состоянию на 17.03.06).

[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, Vol. 3685, 2005.

[McNab, 2004] McNab C. Network Security Assessment. O'Reilly Media Inc, 2004.

[OSVDB, 2006] OSVDB: The Open Source Vulnerability Database [Электронный ресурс] // <http://www.osvdb.org/> (по состоянию на 17.03.06).