

Редактирование в диалоговом окне характеристик субъектов защиты: шифр субъекта, пароль, категория допуска, должность, код классификации. Классификация выделяет подмножество субъектов, имеющих право подписи документов (владельцы объектов), право переписки, право на разрешение доступа к объектам и право ликвидации доступа.

Редактирование в диалоговом окне характеристик объектов защиты: шифр объекта, степень секретности информации, место хранения, субъект-владелец, код классификации, текущий уровень защиты. Понижение уровня секретности объекта происходит из-за естественного старения информации.

Редактирование в диалоговом окне матрицы доступа может осуществляться по двум направлениям: задание шифра субъекта, тогда редактирование видов доступа ко всем его объектам или задание шифра объекта, тогда редактирование видов доступа всех объектов, которые имели различные права доступа к данному объекту.

Управление в диалоговом окне правами доступа субъектов защиты к объектам защиты состоит в определении администратором следующих функций в соответствии с классификацией и категорией допуска субъектов: наделение правами; передача прав; лишение прав; наделение правом владения, наделение правом реализации. Лишение прав субъекта предусматривает удаление из матрицы доступа данного субъекта, что автоматически лишает его всех прав над объектами. Решающие правила по разрешению запросов и изменению состояний системы подробно рассмотрены в [1,2].

Выбор действий над журналом регистрации запросов предусматривает:

- просмотр журнала с установкой фильтра просмотра по дате, по типу транзакций, по имени файла;
- реагирование на попытки несанкционированного доступа неавторизованных пользователей.

В настоящее время сотрудниками Института проблем информатики и управления разрабатывается комплекс программ «Security Access Monitor -монитор безопасного доступа», который может быть применен для систем управления государственными органами с древовидной структурой субъектов и объектов защиты информации, в которых функционирует информация различной степени чувствительности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Горковенко Е.В. Параметры безопасности в многоуровневой модели разграничения доступа.// Известия ТРТУ, тематический выпуск материалов 8-й Международной научно-практической конференции «Информационная безопасность», Россия, – Таганрог: Изд-во ТРТУ, 2006, №7(62), – С 87–91.
2. Горковенко Е.В. Формализованное представление механизмов защиты при мандатном разграничении доступа. Известия Национальной Академии Наук Республики Казахстан, №3, 2006, – С 79–85.

Е.П. Тумоян

Россия, г. Таганрог, Технологический институт ЮФУ

МЕТОДЫ ФОРМАЛЬНОГО МОДЕЛИРОВАНИЯ СЕТЕВЫХ АТАК

Введение

В последние годы вопросы защиты информационных систем от атак приобретают чрезвычайно большое значение. Одним из наиболее важных направлений обеспечения такой защиты является разработка методов и средств, которые позво-

ляют обнаружить факт начала или проведения атаки. К этому числу подобных средств относятся сетевые и хостовые системы обнаружения атак.

Существующие системы обнаружения атак основаны на сигнатурных методах или статистических методах распознавания вредоносных данных.

Перспективные разработки предполагают использование интеллектуальных механизмов для обнаружения атак, например, нейронных сетей, скрытых марковских моделей и нечетких логических правил. Однако при разработке подобных методов мало внимания уделяется исследованию последовательности самих атакующих воздействий, в том числе их анализу и моделированию.

Целью данной работы является разработка модели, которая предоставляет возможности описания атак в условиях динамически меняющихся условий внешней среды, а также метода распознавания атак на основе построенной модели. Построение адекватной и стабильной модели некоторого класса атак позволит существенно повысить точность обнаружения атак, особенно в условиях, когда атакующее воздействие маскируется преднамеренно.

1. Существующие модели атак

В настоящее время существует ряд моделей, позволяющих с разной степенью детализации описать процесс сетевой атаки. Модели используют разную математическую базу, но большинство из них основаны на конечных автоматах и представляют атаку как последовательность состояний автомата.

Этапная модель. Этапная модель предполагает, что атака состоит из нескольких изолированных этапов: этапа исследования, этапа получения управления, этапа расширения привилегий, этапа осуществления вредоносных действий, этап создания потайного хода, этапа заметания следов.

Между этапами могут проходить значительные промежутки времени. Часть этапов могут быть опущены. Данная модель является наиболее распространенной, однако, обладает существенными недостатками:

- 1) Модель не учитывает и не обеспечивает средства по моделированию взаимосвязи между этапами.
- 2) Модель не предоставляет средств для оценки успешности этапа.
- 3) Модель не предоставляет средств для уточнения наличия или отсутствия некоторых этапов.

«Деревья атак». Модель предложена Б. Шнайером в работе [1] в 1999 г. Деревья атаки представляют собой концептуальные диаграммы, которые описывают угрозы системе и возможные атаки, направленные на их реализацию. Модель пригодна для описания атак на любые системы информационного или физического характера. Модель предоставляет возможность для введения оценок каждого шага по некоторым критериям, например, по времени выполнения, числу операций, оценочной стоимости и т.д.

При этом последовательность шагов может быть оценена на основании критериев для каждого шага. В работе [1] приведены примеры оценки деревьев на основе двух критериев, однако, нет принципиальных препятствий для разработки алгоритма многокритериальной оценки.

Данная модель предоставляет большую степень детализации и точности оценок, чем предыдущая. Однако модель не может быть использована для моделирования атак, поскольку не обеспечивает средств динамического моделирования, а также средств для включения в модель условий внешней среды.

Улучшенные деревья атак. Модель описана в работе [2] в 2006 г. Модель опирается на использование деревьев и механизма конечных автоматов для моделирования уязвимостей протоколов и систем. Таким образом, модель представляет собой расширение и уточнение модели деревьев атак. Авторами приводится при-

мер анализа безопасности протокола IEEE 802.11. Данная модель имеет те же недостатки, что и предыдущая.

Графы атак. Модель предложена коллективом исследователей в работе [3] в 2002 г. Видимо, модель графов атак основана на расширении модели деревьев атак. Однако графы атак:

- 1) Являются специализированным средством для описания сетевых атак.
- 2) Для описания используется граф, а не дерево.
- 3) Узлы графа представляют не концептуальные действия, а узлы сети, процессы программы, конфигурационные файлы, участки кода, переменные и т.д.

Моделирование систем на основе графов атак основано на конечных автоматах. Переходы между узлами осуществляются на основе применения детерминированных правил. При этом может учитываться текущее значение некоторых параметров системы, переменных и т.д.

Целью является достижение необходимой вершины. Модель может предусматривать анализ условий, необходимых для достижения цели атаки, поэтому модель может использоваться для оценки безопасности программной системы или компьютерной сети.

Модель получила широкое распространение [3,4], поскольку основана на простой и хорошо исследованной математической базе (конечные автоматы), сама достаточно проста и очевидна. Данная модель была реализована в нескольких инструментальных средствах, например в Lockheed Martin ANGI, а также средстве AttackGraph Tool 0.5 [5].

Недостатком данной модели является то, что, как и в предыдущем случае, она является средством для оценки сложности нарушения безопасности информационной системы, а не моделирования и исследования атак.

Другим существенным недостатком данной модели является применение аппарата конечных автоматов. Модель реальной информационной системы в большинстве случаев не ограничивается моделью автоматов, поскольку включает плохо контролируемые или скрытые факторы.

Interacting State Machines. Модель предложена коллективом исследователей в работе [6] в 2002 г. Модель основана на применении специального типа высокоуровневых конечных автоматов Interacting State Machines (ISM) для моделирования сложных систем. В данной работе ISM применяются для моделирования атакуемого протокола с целью обнаружения ошибок, приводящих к уязвимостям системы, т.е. решаются задачи, существенно отличные от моделирования атак.

2. Предлагаемая модель

Опишем предлагаемую модель следующим образом. Пусть существует множество состояний системы $Q = \{q_i\}$, $i = 0..N$. Тогда представим переход между q_i и q_j как $q_i \rightarrow q_j : \tau(q_i, q_j) = f(P(q_i), \bar{Q}(q_j))$, $\forall i, j$, где $P(q_i)$ - параметры состояния q_i , $\bar{Q}(q_j)$ - в общем случае упорядоченное множество состояний, предшествовавших q_j . Далее сделаем следующие предположения:

1) Пусть всю информацию о состоянии q_i можно представить в виде $P(q_i)$. Тогда $\bar{Q}(q_j)$ содержит информацию только о процессе перехода из состояния q_0 в состояние q_j .

2) Пусть можно найти такие функции $g(\cdot)$ и $h(\cdot)$, что

$$f(P(q_i), \bar{Q}(q_j)) = g(P(q_i)) + h(\bar{Q}(q_j)), \quad \forall i, j.$$

Таким образом, $g(\cdot)$ можно рассматривать как модель, характеризующую переходы из состояния в состояние, а $h(\cdot)$ - модель, характеризующую историю системы.

3) Для того, чтобы учесть изменения вносимые переходом системы в некоторое состояние q_i введем понятие *влияние состояния*. Влияние состояния $A(q_i)$ – это изменение, вносимое в систему переходом системы в данное состояние, в процессе пребывания системы в данном состоянии или в результате выхода из данного состояния. При этом $P'(q_i) = P(q_i) + A(q_i)$ и $P(q_{i+1}) = P'(q_i) + H'(q_i)$, где $A(q_i)$ – влияние состояния, $H'(q_i)$ – изменение, вносимые внешними факторами. Учитывая приведенные определения, пример модели из пяти состояний и шести переходов можно изобразить, как показано на рис.1.

Можно предложить различные варианты выбора $g(\cdot)$ и $h(\cdot)$. Для определенности в данной работе предлагается следующее:

1) Функция $g(\cdot)$ представляют собой вероятностные нейронные сети (Probabilistic Neural Networks, PNN) в режиме классификации. Данный тип нейронных сетей позволяет проводить классификацию данных на основе оценки вероятности принадлежности данных к некоторому классу. Как и другие типы нейронных сетей, PNN должны быть обучены на классификацию данных, однако, время обучения PNN чрезвычайно мало.

2) Значение $A(q_i)$ вычисляется на основе многослойных нейронных сетей прямого распространения с гладкими активационными функциями (Multilayer Perceptrons, MLP). Данный тип нейронной сети позволяют приблизить любую гладкую функцию от входных аргументов. Недостатком данной сети является большое время обучения.

3) Функция $h(\cdot)$ представляет собой расчет вероятностей на основе Марковских моделей (Markov models). Данный метод позволяет быстро построить долговременную вероятностную модель системы и оценить вероятность некоторого состояния. Другим возможным способом представления $h(\cdot)$ могут стать вероятностные суффиксные деревья (Probabilistic suffix trees, PST), которые обеспечивают подобные возможности.

Возвращаясь к задаче моделирования атак, опишем приведенные величины.

Состояние представляет собой этап атаки. Формальные признаки отдельного этапа атаки – законченное воздействие на атакуемую систему. Пример – переполнение буфера для захвата управления, расширение привилегий и т.д. Воздействие состояния – влияние перехода в некоторое состояние на переменные системы. В целях упрощения расчета при описании воздействия состояния имеет смысл использовать модель общей памяти, т.е. состояние системы представляется в виде глобального пула переменных, который модифицируется атакующими воздействиями в ходе атаки. Переход представляет собой вероятностную взаимосвязь между различными вариантами атаки.

Функция $g(\cdot)$ обеспечивает получение номера и вероятности следующего состояния по переменным системы. Эта функция учитывает *кратковременные изменения в атаке*, и меняется на основе проверки локальных условий, например, «удалось ли получить управление?», «удалось ли расширить привилегии?» и т.д. Данная функция должна быть рассчитана индивидуально для каждого этапа атаки при создании каждого сценария.

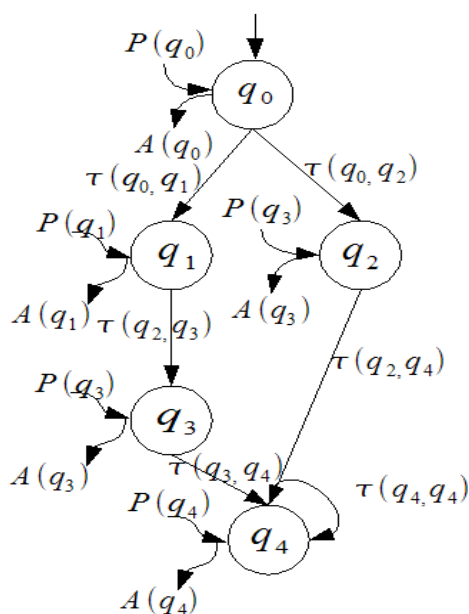


Рис. 1. Пример предлагаемой модели

Однако, как отмечалось ранее, вероятностные нейронные сети (PNN) допускают чрезвычайно быстрое обучение. $A(q_i)$ – предложенный способ вычисления $A(q_i)$ позволяет абстрагироваться от фактической реализации атаки, которая может быть существенно различной (например, применение набора инструкций процессора, команд интерпретируемого языка, получение вредоносного пакета и т.д.) и оценивать изменения в различных типах переменных системы. Данная функция соответствует *описанию действия этапа атаки* на систему. Функция инвариантна к сценарию атаки, в котором используется этап. Создание данного преобразования на основе многослойных перцептронов является наиболее сложной и ресурсоемкой задачей, однако выполняется один раз для каждого этапа атаки. Функция $h(.)$ – учитывает *долговременные изменения* в ходе атаки на основе вероятностных параметров. Данная функция должна быть рассчитана для каждого сценария атаки. При этом выбранные методы (марковские модели и «суффиксные деревья») позволяют производить построение данной функции чрезвычайно быстро.

Заключение

Предложенная в работе модель обеспечивает получение описания сценариев различных атак с использованием общей понятийной базы и общего метода моделирования. Как было упомянуто ранее, модель обеспечивает учет параметров, которые динамически меняются в ходе выполнения сценария атаки, а также параметров, которые изменяются самим атакующим воздействием.

Дальнейшим продолжением данной работы станет разработка методов выполнения преобразований для предложенной модели, например, сложения, вычитания, упрощения, сравнения и т.д. Разработка таких методов позволит построить эффективные средства обнаружения атак как ранее известных, так и новых. Основной проблемой при этом является сбор данных о сценарии проведения атаки в виде, пригодном для использования в данной модели. В настоящее время базы данных атак, содержащие такие данные, в открытом доступе не представлены.

Однако существует ряд проектов по унификации описания и сбору унифицированных данных атак, например, Common Weakness Enumeration. Развитие таких проектов, видимо, позволит получить необходимую информацию о проведении атак.

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// Lecture Notes in Computer Science, 2002, № 2502. P. 212–228.

Д.В. Мордвин, Е.С. Абрамов

Россия, г. Таганрог, Технологический институт ЮФУ

РАЗРАБОТКА ИНСТРУМЕНТАЛЬНЫХ СРЕДСТВ ДЛЯ МОДЕЛИРОВАНИЯ ЛВС

На данный момент в свободном распространении не существует программ моделирования сетей ТСП/Р для целей ознакомления и обучения студентов принципам работы сети, стека протоколов ТСП/Р, сетевых служб, сетевых атак. Существуют программы для рисования структуры сети и моделирования сети с целью ее оптимизации, но этого не достаточно.

На данный момент изучение логики работы сети, сетевых протоколов, сетевых атак происходит в теории и при помощи так называемых логов от работы специальных утилит, например tcpdump.

В связи с этим встала задача разработать программу, которая бы позволяла не только моделировать ЛВС, но и моделировать пакеты, сетевой трафик, работу протоколов, служб, сетевые атаки.

Моделирование сетевых устройств

В программе доступно пять типов устройств: компьютеры с сетевой картой, серверные станции, концентраторы, коммутаторы, маршрутизаторы.

Каждое из этих устройств представляет собой отдельный объект, который можно помещать на форму для создания сети, перемещать по форме, соединять с другими устройствами. С каждым из устройств связаны его параметры, которые можно задавать после помещения объекта на форму.

Для каждого устройства смоделированы основные логические свойства, которые имеют реальные устройства такого типа.

Программа не моделирует реальные физические свойства устройств, такие как скорость передачи пакетов, потери пакетов. Моделируются только те свойства, которые помогут глубже понять логику работы сети.