Проект 1994Р: Формальные методы защиты информации в компьютерных сетях

1 Название проекта/ Номер годового отчета

Задача 1: Разработка математической модели, архитектуры и программного прототипа системы моделирования удаленных атак на компьютерные сети.
Отчет №1

2. Головной институт

Санкт-Петербургский институт информатики и автоматизации Российской академии наук

3. Институты-участники

Нет

4. Руководитель , номер телефона, факса, адрес электронной почты

Городецкий Владимир Иванович, (812)-323-3570, (812)-328-0685, gor@mail.iias.spb.su

5. Дата начала осуществления, продолжительность проекта

1 декабря 2000, 27 месяцев

6. Краткое описание плана работ: цель, предполагаемые результаты, научно-технический подход

Краткий план работ

А-1. Разработка концептуальных описаний представительного множества распределенных атак на макро уровне и их моделей.	1-3 кварталы
Промежуточный отчет #1, представляющий результаты исследований по задаче А-1.	3 квартал
А-2. Разработка формальных моделей сетевых атак.	2-3 кварталы
Промежуточный отчет #2, представляющий результаты исследований по задачам А-1 и А-2.	4 квартал
А-3. Разработка объектно-ориентированного проекта программного прототипа системы "Симулятор атак".	4-6 кварталы
Представление статьи в международный журнал.	5 квартал
Промежуточный отчет # 2, представляющий результаты исследований по задаче А-3.	6 квартал
А-4. Разработка объектно-ориентированного проекта программного прототипа системы "Симулятор сетевых атак".	6-9 кварталы
Демонстрация программных компонент, которые будут использованы в прототипе Симулятора атак (По согласованию с US AFRL/ID.).	9 квартал
Итоговый отчет и общее заключение по задаче 1	9 квартал

Примечание: Строки таблицы, залитые серым цветом, отвечают исследованиям, запланированным на первый год работы. Задача А.3 в этот период должна быть решена только частично.

Цель проекта

Целью данной задачи проекта является разработка формальной модели и программного обеспечения для моделирования широкого спектра распределенных атак, а также исследование ее возможностей и полезности применительно к решению задач защиты компьютерных сетей.

Ожидаемые результаты

1.Спецификацию представительного множества удаленных атак, базирующуюся на сценариях;
2. Методики и алгоритмы восстановления формальных грамматик, задающих модели атак различных классов;
3. Стохастические модели фрагментов атак на микро-уровне;
4. Объектно-ориентированный проект программного прототипа системы моделирования атак;
5. Программный прототип системы моделирования атак и результаты исследования на основе компьютерного моделирования его работы с оценкой полезности его практического использования.

Научно-технический подход

Распределенная атака планируется на макро-уровне в виде частично упорядоченного множества шагов, задающих сценарий. Каждый шаг направлен на достижение частной цели и соответствует некоторой частной атаке.. При реализации конкретной атаки некоторые шаги выбранного сценария могут быть успешными, а другие – нет. Эти шаги могут быть реализованы в различном порядке, многократно повторяться и выполняться с различных удаленных компьютеров. Они могут быть направлены на различные ресурсы компьютерной сети. Для реализации каждого шага сценария атаки используются операции нижнего уровня в виде последовательности команд.

В соответствии с названными особенностями приложения, используется следующий подход.

На макро-уровне используется формализация сценариев в терминах структуры формальных грамматик, связанных операцией подстановки. Каждая реализация сценария рассматривается как последовательность шагов атаки на макро уровне. Каждая такая последовательность рассматривается как “слово”, принадлежащее формальному языку, который формально задается посредством формальной грамматики. Множество "слов" такого "языка" может быть использовано для регенерации (восстановления) грамматики формальными методами. Однако в настоящее время используется экспертный метод восстановления грамматики, что обусловлено недостатком экспериментальных данных и наличием информации о структуре атак, полученной экспертным путем. Проведенные анализ и полученные результаты показывают, что адекватное описание сценариев атак может быть выполнено в терминах стохастических (атрибутных) *LL2)* право-рекурсивных грамматик

Второй уровень моделирования соответствует спецификации атак на микро уровне. Каждый шаг сценария, заданный на макро уровне, состоит из последовательности различных событий (например, системных вызовов) микро уровня. Событие в этой последовательности реализует некоторое конкретное действие или команду злоумышленника, которое в разрабатываемой модели относится к микро уровню. Моделирование этого уровня также может быть выполнено в терминах формальных грамматик с подстановкой в листьях дерева вывода последовательностей, отвечающих низкоуровневому описанию действий злоумышленника.

7. Ход выполнения технических работ за первый год (для годовых отчетов за второй год)

8. Ход выполнения технических работ за рассматриваемый год

Ход выполнения работ полностью соответствует плану работ как по содержанию, так и по срокам завершения предусмотренных этапов работ.

Основные достижения за прошлый год

Основные достижения за прошлый год связаны с решением запланированных задач. Эти задачи и полученные по ним результаты перечисляются ниже.

1. Разработка концептуальных описаний представительного множества распределенных атак на макро уровне и их моделей.

2. Разработка формальных моделей сетевых атак.

3. Разработка объектно-ориентированного проекта программного прототипа системы "Симулятор атак".

Основные результаты, полученные в течение первого года исследований, таковы.

1. Проведен анализ и классификация известных к настоящему времени атак на отдельные компьютеры, а также на компьютерные сети. Анализу подвергнуто большое количество атак. Разработана таксономия атак, которая положена в основу классификации, использованной далее при разработке представительного множества атак для последующего моделирования.

2.Разработано концептуальное описание представительного множества атак, которые являются компонентами сценариев распределенных атак. В частности, оно включает в себя компоненты сетевых атак следующих классов:

(1) анализ сетевого трафика,
(2) сканирование сети,
(3) подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа,
(4) внедрение ложного объекта в сеть,
(5) отказ в обслуживании,
(6) неавторизованный доступ с удаленного хоста посредством подбора пароля,
(7) неавторизованное повышение привилегий доступа,
(8) удаленный запуск приложений.

Каждый из перечисленных классов атак описан как множество допустимых последовательностей шагов (этапов), определяющих класс атаки на макро и микро уровне.

Разработана двухуровневая концептуальная модель атак. На макро-уровне модель задает сценарии атак различного уровня детальности. Даже единичный прецедент такого сценария позволяет эксперту идентифицировать намерения атакующего, особенности выполнения атаки, ее варианты и переменные параметры, ведущие к той же самой цели. Каждый сценарий описывается множеством допустимых последовательностей шагов, определяющих класс атак на макро-уровне. На микро-уровне каждый шаг сценария (макро-уровня) представляется последовательностью событий. Этими событиями могут быть конкретные команды операционной системы, вызываемые стандартные приложения и программы атакующего ("эксплойты") с конкретными параметрами вызова.

Для сценариев каждого класса атак описаны варианты их реализации в частных формах, отвечающих вариантам математического обеспечения, установленного на компьютерах атакуемой сети.

Сценарии атак класса “*Анализ сетевого трафика*” реализуются в виде последовательности следующих этапов: определение места (множества мест) в сети, с которого следует осуществлять прослушивание; определение анализируемых уровней сетевых протоколов (по системе OSI), а также самих протоколов; определение активного сетевого оборудования в сети и механизмов его работы; определение программных средств анализа и ОС, под управлением которой этот анализ будет проходить; настройка программных средств и выработка правил (паттернов), на основании которых будет происходить фильтрация информации; анализ и выбор средств, маскирующих атакующего; включение в сеть и запуск всех программных средств (как анализирующих сетевой трафик, так и маскирующих атакующего); получение и анализ (фильтрация) проходящего сетевого трафика; отключение от сети; анализ, расшифровка, и классификация полученной информации атакующим.

Наиболее важные стадии сценариев атак класса “*Сканирование сети*” представлены так: выбор компьютера-посредника и подключение к нему; определение компьютеров, присутствующих в атакуемой сети путем рассылки запросов по всему множеству интересующих адресов; исследование структуры атакуемой сети путем последовательной отправки специализированных тестовых пакетов различным компьютерам и анализа ответов, а также маршрутов пакетов; определение служб, запущенных на выбранном компьютере, путем последовательного обращения ко всем портам (TCP и UDP) из интересующей группы; сбор дополнительной информации об атакуемой сети;

Модели атак класса “*Подмена доверенного объекта сети*” включают реализацию следующих стадий: подготовительный этап, связанный с анализом атакуемых объектов и подменой информации (например, URL-адреса) на сервере; прослушивание сети; отправка запроса; отправка ответа; выполнение команд на атакованном хосте; прием и анализ перехваченной информации; воздействие на перехваченную информацию; передача перехваченной информации (возможно измененной или подмененной); распространение атаки на другие объекты.

Общий сценарий класса атак “*Внедрение ложного объекта в сеть*” состоит из следующих этапов: изучение сегмента сети атакуемого; прослушивание сети; отправка ложного сообщения

(или шторма сообщений); прием и анализ перехваченной информации атакующим или “обманутым” сервером; воздействие на перехваченную информацию; передача перехваченной информации (возможно измененной или подмененной).

Модель реализации атак класса “*Отказ в обслуживании*” содержит такие наиболее важные обобщенные этапы: исследование сети; внедрение на вспомогательные (промежуточные) хосты агентов-менеджеров и агентов-демонов; посылка агентами-демонами сообщений агентам-менеджерам (например, о состоянии); посылка злоумышленнику информации от агентов-менеджеров о состоянии агентов-демонов; посылка хостом злоумышленника команд агентам-менеджерам; посылка агентами-менеджерами команд агентам-демонам; посылка хостом злоумышленника (или хостом, используемым злоумышленником) специально созданного пакета на промежуточный хост (множество промежуточных хостов); промежуточный хост (множество промежуточных хостов) получает пакет и посылает ответный пакет на хост – цель атаки; хост – цель атаки получает пакет и посылает ответный пакет промежуточному хосту; посылка хостом злоумышленника (или хостом, используемым злоумышленником) специально созданного пакета (серии пакетов, фрагмента пакета) на хост – цель атаки.

Сценарии атак класса “*Неавторизованный доступ с удаленного хоста посредством подбора пароля*” характеризуются выполнением следующих фаз: получение информации об используемой системе аутентификации; получение информации о пользователях системы; перехват зашифрованных (хешированных) паролей; получение базы зашифрованных (хешированных) паролей; однократный ввод пароля в режиме *on-line*; многократный ввод пароля в режиме *on-line*; подбор пароля в режиме *off-line* путем перебора большого числа паролей.

Сценарии атак класса “*Неавторизованное повышение привилегий доступа*” включают следующие *этапы*: анализ объектов атаки; подготовка кода; внедрение кода; внедрение параметров (параметризация кода); передача управления коду.

Наиболее важные обобщенные этапы сценариев атак класса “*Удаленный запуск приложений*” таковы: исследование системы; внедрение в систему чуждых программного кода или текстов программ; несанкционированный доступ к ресурсам системы; запуск и использование вспомогательных программных средств, легально присутствующих в атакуемой системе; запуск враждебной программы; активизация кода для выполнения требуемой функции и ее последующее выполнение; передача информации нарушителю; уничтожение следов пребывания; самовоспроизведение враждебного кода.

3. Проведено тщательное изучение формальных моделей, которые потенциально могут быть использованы в качестве формальных механизмов для формального описания и последующего компьютерного моделирования распределенных атак. Анализ показал, что использование формальных грамматик позволяет адекватно формализовать описание атак наилучшим образом поскольку формальные грамматики применяются для объектов реального мира регулярной структуры. В частности, они позволяют построить адекватное формальное описание сценариев достаточно сложных атак. Кроме того, грамматики могут быть использованы и в другой роли: они могут использоваться при распознавании атак, если ее рассматривать как задачу синтаксического анализа цепочек известной структуры.

4. Проведен подробный анализ методов восстановления грамматик описывающих атаки на компьютерные сети по прецедентам (примерам) атак. Проведен тщательный анализ известных методов восстановления грамматик и возможностей их использования в задачах моделирования. Формально, задача восстановления грамматик состоит в построении алгоритма восстановления синтаксической структуры конечного множества "слов" языка описания атак и дополнительного языка, т.е. по примерам и контр-примерам. Аналогичным образом методы восстановления грамматик используются также и для восстановления структур сценариев распределенных атак. При этом можно использовать три подхода: 1) использованием индуктивных алгоритмов; 2) с привлечением экспертов, обладающих знаниями о намерениях злоумышленников и возможных путей реализации ими этих намерений, и 3) использованием комбинации двух вышеназванных подходов.

Выбрано две группы алгоритмов восстановления грамматик: (1) перечислительный алгоритм восстановления грамматик и (2) алгоритм индуктивного восстановления. Среди них, индуктивные алгоритмы представляется более адекватным для решаемой задачи, в частности, для восстановления грамматики на основании положительных примеров удобен метод Фельдмана. Суть этого метода в построении не-рекурсивной грамматики, которая в точности представляет

множество примеров, с последующим введением рекурсий, которые позволяют генерировать все экземпляры тренировочной выборки, а также бесконечное множество других цепочек.

Для верификации свойств такого алгоритма было рассмотрено несколько конкретных задач восстановления грамматик с помощью метода Фельдмана применительно к данным об атаках. Эти примеры использованы для восстановления грамматик, формализующих модели следующих типов атак: сканирование портов с целью идентификации хоста; сканирование сети для идентификации сервисов; сканирование с целью определения типа операционной системы; сканирование для определения разделяемых ресурсов; сканирование для определения имен пользователей хоста; сканирование с целью определения работающих приложений и заголовков сообщений; деятельность по доступу к ресурсам сети, а также атака с целью достижения отказа в обслуживании.

Разработаны также конкретные модели атак на основе использования экспертных знаний. Результаты показывают, что предложенный подход удобен для формального описания атак. Результирующие грамматики могут использоваться для генерации обучающих выборок широкого спектра атак.

5. Разработана многоуровневая формальная модель представительного множества атак, описанная в терминах семейства взаимодействующих грамматик, связанных операцией подстановки в грамматиках. Эта модель позволяет описывать формально большое разнообразие распределенных атак на различных уровнях детальности. Эта модель включает спецификации всех основных компонент в частности:

Базовые понятия, описывающие атаку. Они включают в себя описание сценария распределенной атаки и намерений злоумышленника. В разработанной модели используется так называемый "*подход, фокусирующийся на намерениях злоумышленника*" Это означает, что базовые понятия структурируются в соответствии с намерениями злоумышленника, а все другие понятия ассоциируются с такой структурой.

Онтология понятий предметной области "Атаки на компьютерные сети". Понятия этой онтологии имеют те же имена, что и символы грамматики, а их интерпретации в онтологии формируют интерпретацию символов грамматик, описывающих атаки Таким образом, последовательность символов, формализующих сценарии атак, являются последовательностями идентификаторов понятий онтологии.

Формальная модель атакуемой сети. В модели атак атакуемая сеть рассматривается как внешняя среда, которая реагирует на действия злоумышленника. *Основными параметрами хостов* в модели сети являются: IP-адрес, маска сетевого адреса, тип и версия ОС, идентификаторы пользователей, имя в домене, пароль доступа к хосту, идентификатор защиты (SID) пользователя, параметры домена, активные порты (сервисы) хоста (используемый сервис, задействованный TCP и UDP порт), запущенные приложения, параметры защищенности, разделяемые ресурсы, доверенные хосты и ряд других параметров.

С точки зрения программной реализации распределенная атака рассматривается как множество скоординированных действий пространственно распределенных злоумышленников. Этот уровень модели описывается как многоагентная система. Для нее разрабатывается архитектура, в которой каждому злоумышленнику ставится в соответствие программный агент, при этом все такие агенты одинаковы по своим функциональным возможностям. При реализации атак агенты взаимодействуют между собой на основе обмена сообщениями. Эти сообщения специфицируются на языке коммуникаций KQML,который является стандартом DARPA. Содержание сообщения представляется на языке XML. Проектирование и программная реализация такой многоагентной системы выполняется в среде инструментального средства Multi-Agent System Development Kit (MASDK), разработанного авторами данного исследования.

6. Проведено объектно-ориентированное проектирование макро-уровневых компонент Симулятора атак. В частности, разработаны спецификации для реализации следующих компонент:

(1) модели действий злоумышленника;

(2) моделей атакуемой компьютерной сети и хостов;

(3) модели вычисления вероятностей успешного выполнения атак (действий) злоумышленником;

(4) модели реакции хостов на действия злоумышленника.

В соответствии с рабочим планом объектно-ориентированное проектирование остальных компонент Симулятора атак должно быть закончено к концу 6 квартала.

9. Существующее положение дел с выполнением технических работ

Ход выполнения работ полностью соответствует предусмотренному плану и в коррекции не нуждается.

10. Сотрудничество с зарубежными партнерами

В соответствии с планом работ партнеру представлены два промежуточных отчета (1 июня 2001 и 1 декабря 2001), в которых полностью представлены соответствующие результаты исследований.

Исполнители проекта совместно с представителем партнера участвовали в Европейской школе по многоагентным системам. В марте 2001 была организована командировка руководителя проекта в организацию партнера для обсуждения предстоящих исследований. Представитель партнера посещал Институт в мае 2001 г. Планируется большой семинар по обсуждению результатов исследований за первый год в феврале 2002 в организации партнера в США.

11. Выявленные проблемы и предложения относительно их устранения

Нет

12. Перспективы дальнейшего развития разработанной технологии/научного исследования

Будут обсуждаться на встрече с партнеров в феврале 2002 г.

Приложение 1. Наглядные материалы, прилагаемые к основному тексту

Нет

Приложение 2. Другая дополнительная информация к основному тексту

Краткое содержание Промежуточных отчетов, представленных партнеру

Промежуточный отчет №1

Промежуточный отчет №2

Приложение 3. Резюме статей и докладов, опубликованных за рассматриваемый год

1. В.И.Городецкий, И.В.Котенко. Модели атак на компьютерные сети, основанные на использовании формальных грамматик. В трудах Международной конференции по мягким вычислениям и измерениям (*SCM-01*), Санкт-Петербург, Россия, стр. 212-216, 2001.

   Абстракт. В настоящей работе дается представление о предлагаемых формальных моделях атак, основанных на использовании формальных грамматик. Эти модели предназначены для реализации в разрабатываемой системе моделирования атак. Проводится анализ атак на компьютерные сети. Предлагается двухуровневая концептуальная модель атак. На первом (макро) уровне задается общий сценарий атаки. Каждый сценарий описывается множеством допустимых последовательностей шагов, определяющих класс атак на макро-уровне. Второй (микро) уровень определяет более детальную спецификацию атаки. Каждый шаг сценария (макро-уровня) на микро-уровне состоит из последовательности событий. Этими событиями являются конкретные команды операционной системы, вызываемые стандартные приложения и программы атакующего (эксплоиты) с конкретными параметрами вызова. На основе использования стохастической контекстно-свободной грамматики дается описание обобщенного сценария атаки. Представляется дерево разбора этой грамматики.

2. В.И. Городецкий, О.В. Карсаев, И.В.Котенко, А.В. Хабалов. MAS DK: инструментарий для разработки многоагентных систем и примеры приложений. В трудах международной конференции "Искусственный интеллект в XXI веке" (*ICAI'2001*), Изд. Физико-математической литературы, Москва, стр. 249-262, 2001.

   Абстракт. В статье рассматривается предлагаемая авторами технология и реализующий эту технологию инструментарий разработки многоагентных систем MASDK. Данный инструментарий базируется на использовании набора инвариантных компонентов, объединенных в виде “Типового агента”. Процесс разработки многоагентной системы рассматривается как развитие “Типового агента” в классы специфических агентов приложения. Формирование классов агентов приложения предполагает определение сценариев их поведения и схемы взаимодействия. Совокупность последних формируется и хранится в “Системном ядре” – специализированной базе данных ИР МАС. Статья также содержит краткое описание трех разрабатываемых с помощью ИР МАС прототипов прикладных систем: (1) планирования операций и составления расписаний, (2) извлечения закономерностей из экспериментальных данных, (3) обнаружения вторжений в компьютерные сети.

3. Городецкий В.И., Карсаев О.В., Котенко И.В., Хабалов А.В. Инструментарий для разработки многоагентных систем. International Workshop of Central and Eastern Europe on Multi-agent Systems *(CEEMAS-2001),* Krakow, Poland, September 2001 (Будет опубликована также в серии "*Lecture Notes In Artificial Intelligence*" в 2002).

Абстракт. В статье представляется разработанная технология и инструментальное программное средство для проектирования и разработки многоагентных систем, основанных на знаниях. Программный инструментарий включает две компоненты: "Типовой агент" и "Набор инструментов для разработки многоагентных систем". Первая компонента представляет собой набор классов Visual C++ и Java, которые инвариантны по отношению к приложениям и допускают поэтому повторное использование. Вторая компонента состоит из нескольких специализированных редакторов, снабженных понятным пользовательским интерфейсом, которые используются для формального описания типовых классов агентов и типовых структур данных, формирующих конкретное приложение из типового агента. Это формальное описание затем инсталлируется на конкретную компьютерную сеть. Разработанная технология и набор инструментов для разработки и программной реализации многоагентных систем использованы для создания ряда приложений из области защиты компьютерных сетей, планирования операций и извлечения знаний из данных.

4. Городецкий В.И., Котенко И.В., Манько Е.В. Моделирование распределенных атак на компьютерные сети. В материалах II-й Межрегиональной конференции "Информационная безопасность регионов России", (*ИББР-2001*), Санкт-Петербург, Россия, 26-28 ноября 2001, стр. 56-57.

Абстракт. Разработана формальная модель распределенных атак, которая построена как иерархия контекстно-свободных атрибутных стохастических грамматик, связанных с помощью операции подстановки. Концептуальную основу модели составляет разработанная авторами онтология предметной области "Сетевые атаки на компьютерные сети". Содержательно каждому из узлов онтологии отвечает или подцель, которую пытается достичь злоумышленник, или набор действий, с помощью которых некая подцель может быть достигнута. В программном инструментарии процессы порождения атак интерпретируются алгоритмически с помощью разработанного множества взаимодействующих автоматов. Инструментарий включает также модель атакуемой сети, в которой реализована некоторая политика безопасности, и реакции сети на действия атакующего. Программная система моделирования атак реализуется как многоагентная система, в которой каждый из злоумышленников моделируется агентом, а компьютерная сеть рассматривается как внешняя среда. В процессе атаки агенты координируют свои действия на основе обмена сообщениями.

Менеджер задачи
профессор
В.И.Городецкий