1 Название проекта/ Номер годового отчета

Проект 1994Р: Формальные методы защиты информации в компьютерных сетях

Задача 1: Разработка математической модели, архитектуры и программного прототипа системы моделирования удаленных атак на компьютерные сети.
Отчет №2

2. Головной институт

Санкт-Петербургский институт информатики и автоматизации Российской академии наук

3. Институты-участники

Нет

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

Котенко Игорь Витальевич, (812)-323-3570, (812)-328-0685, ivkote@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 # 3, 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, показанные серым цветом, отвечают исследованиям, запланированным на второй год работы. Задача А.4 в этот период должна быть решена только частично.

Цель проекта

Целью задачи 1 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

Основным ожидаемым результатом будет формальный подход, модель, архитектура и программный прототип системы моделирования атак на компьютерные сети. Детализация этих результатов может быть представлена следующим образом:

1. Спецификация представительного множества удаленных атак, основанная 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. Проведенный 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)

Ход выполнения работ первого года исследований полностью соответствовал плану работ как по содержанию, так и по срокам завершения предусмотренных этапов работ.

Основные достижения за первый год исследований

Основные достижения 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. 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) использование индуктивных алгоритмов; (2) привлечение экспертов, обладающих знаниями о намерениях злоумышленников и возможных путей реализации ими этих намерений, и (3) использование 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, последовательности 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.

8. Ход выполнения технических работ за рассматриваемый год

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

Основные достижения за рассматриваемый год

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

1. Разработка объектно-ориентированного проекта программного прототипа системы "Симулятор атак" (системы моделирования атак).

2. Разработка программного прототипа системы "Симулятор атак" (системы моделирования атак).

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

1. *Уточнен используемый подход к моделированию атак на компьютерные сети.*

Концептуальное исследование атак позволило выявить следующие *особенности планирования и выполнения атак*, влияющие на выбор формальной модели атак и проектирование системы моделирования атак:

- атака направлена на конкретный объект и, как правило, имеет вполне определенную цель;
- намерение атакующего может быть представлено в терминах частично упорядоченного множества намерений более низкого уровня и действий, которые могут быть реализованы различными способами; развитие атаки в значительной степени определяется реакцией атакуемой компьютерной сети, выбор продолжения атаки почти всегда недетерминирован; сценарий развития атаки не может быть задан заранее, так как любая атака зависит от множества неопределенностей: неопределенности выбора намерения атакующего и объекта атаки; неопределенности выбора сценария атаки, реализующего выбранное намерение; неопределенности реакции на атаку компьютерной сети и др.

Отличительными чертами разработанного подхода, влияющими на выполнение объектно-ориентированного проекта системы моделирования атак, являются следующие:

- моделирование атаки основывается на задании намерений злоумышленника и спецификации объектов атаки;
- многоуровневая спецификация атаки представляется в следующей последовательности (от верхнего к нижним уровням): “задача атаки (цель) и объект атаки → структурированные намерения злоумышленников → действия злоумышленников → реакция атакуемой компьютерной сети”;
- структурирование модели атаки базируется на использовании онтологии предметной области;
- для формальной спецификации сценариев атаки и ее компонент (“простых атак”) используются атрибутные стохастические *LL*(*2*) контекстно-свободные грамматики, что означает, что цепочки грамматик генерируются слева направо, сверху вниз с неопределенностью выбора подстановки для второго символа включительно;
- для задания многоуровневой структуры атак используются операции подстановки формальных грамматик;
- интерпретация формальных грамматик осуществляется на основе автоматов;
- генерация действий злоумышленников происходит в зависимости от реакции атакуемой сети в реальном масштабе времени.

Более точно определенная концептуальная модель атак на компьютерные сети позволила разработать объектно-ориентированный проект программного прототипа системы моделирования атак на компьютерные сети.

2. В целях разработки объектно-ориентированного проекта программного прототипа системы моделирования атак на компьютерные сети и его реализации *разработаны и использованы технология и программный инструментарий, названный Multi-agent System Development Kit (MAS DK)*. Этот инструментарий реализован на базе Visual C++ 6.0, JAVA1.3 и XML.

3. *Разработан объектно-ориентированный проект программного прототипа системы “Симулятор атак” (системы моделирования атак).*

Следующие *основные компоненты программного прототипа* были определены в объектно-ориентированном проекте и реализованы:

(1) *Компонента задания онтологии предметной области* (*DomainOntology*).Она предназначена для задания и хранения понятий, атрибутов понятий и значений атрибутов понятий предметной области моделирования атак на компьютерные сети. Заполнение онтологии предметной области осуществляется на этапе проектирования с использованием редактора онтологии MAS DK. При заполнении онтологии через пользовательский интерфейс заносятся и модифицируются понятия (классы) онтологии, атрибуты понятий (классов), а также мета-классы, объединяющие понятия в группы (в *DomainOntology* они не используются).

(2) *Компонента реализации множества формализованных сценариев атак в виде семейства автоматов* (*AttackModel*). Посредством спецификации так называемых “прикладных” автоматов *AttackModel* задает множество выполняемых формализованных сценариев атак. Компонент используется для спецификации множества различных классов атак в виде семейства автоматов. Состояния и переходы между состояниями являются основными

элементами автомата. Схема описания каждого автомата включает следующие элементы: название автомата, его предназначение и общее описание; идентификатор узла онтологии атак, которому соответствует автомат; диаграмма автомата; основные параметры автомата; параметры переходов; условия переходов; и скрипты.

(3) *Компонента интерпретации семейства автоматов* (*Engine*). Данная компонента реализует механизмы работы с "прикладными" автоматами, задаваемыми в компоненте *AttackModel*, и осуществляет управление их поведением на основе использования инвариантного мета-автомата. Функционирование прикладных автоматов происходит под управлением инвариантного мета-автомата. Мета-автомат создает экземпляры прикладных автоматов, преобразует скрипты автоматов во внутреннее представление, обеспечивает связь скриптов автоматов с компонентой *DomainOntology* и выполняет их, осуществляет передачу управления между прикладными автоматами и удаляет экземпляр прикладного автомата после завершения его функционирования.

(4) *Корневая компонента задания спецификации задачи атаки и поддержки взаимодействия с основными компонентами прототипа* (*AgentLib*). Компонента *AgentLib* является своего рода "шлюзом", связывающим компоненту *Engine* с программными компонентами, реализующими конкретные прикладные задачи.

(5) *Компонента интерфейса пользователя для отображения спецификации задачи атаки* (*TargetObjectiv*). Спецификация атаки включает намерение, адрес атакуемого хоста (сети), объект атаки, информацию, уже известную атакующему об объекте атаки (хосте или сети).

(6) *Компонента определения вероятности перехода в следующее состояние автомата* (*SMProb*). Компонента состоит из трех классов: (а) *Transition,* ответственного за каждый отдельный (уникальный) переход; (б) *Transitions,* содержащего вероятностную группу, состоящую из экземпляров класса *Transition*, отвечающих за каждый отдельный переход внутри этой вероятностной группы; (в) *Prob_DB,* обеспечивающего работу с таблицей *SrcProb*, взаимодействие с классом вероятностной группы и классами отдельных переходов внутри вероятностной группы.

(7) *Компонента интерфейса пользователя для отображения процесса реализации атаки* (*AtlogView*).

Компоненты *AgentLib, TargetObjectiv, SMProb* и *AtlogView* являются программными реализациями прототипа на языке VC++. Компоненты *DomainOntology* и *AttackModel* представляют собой семантические составляющие прототипа. Они описаны в терминах структур, предоставляемых средой MAS DK. Объектно-ориентированное описание программной реализации автоматной модели и взаимодействия автоматной модели с предметной областью вынесено в компоненту *Engine*.

4. Базируясь на решениях, полученных при разработке объектно-ориентированного проекта, *реализована первая версия программного прототипа системы моделирования атак на компьютерные сети*.

Разработанный объектно-ориентированный проект показал, что дальнейшая разработка программного прототипа системы моделирования атак на компьютерные сети повлечет ряд существенных изменений.

Все *доработки и изменения программного прототипа* по времени их реализации разбиты на две категории:

(1) первоочередные (ближайшие) и

(2) стратегические (дальнейшей перспективы) (в большинстве решений эти изменения выходят за рамки настоящего проекта).

К *первоочередным* отнесены следующие решения:

- включение в прототип возможности запуска процесса моделирования атак, когда известна часть данных об атакуемой сети;
- включение в прототип возможности спецификации конкретного объекта атаки (файлы, ресурсы, запущенные приложения, учетные записи и т.д.);
- расширение классов атак;
- реализация некоторых классов действий атакующего на микро-уровне;
- реализация учета структуры атакуемой сети и специфики хостов при моделировании атаки;
- задание структуры атакуемой сети (сетей) с помощью пользовательского интерфейса;

- введение дополнительной спецификации хостов в атакуемой сети (сетях) для различения типа хоста.

К основным *стратегическим* решениям по развитию прототипа относятся следующие:

- использование в качестве объекта атаки реальной сети;
- использование при реализации сценариев атак реальных утилит и эксплоитов;
- реализация системы моделирования атак как команды агентов-хакеров, совместно решающих общую задачу.

5. *Реализована вторая версия программного прототипа системы моделирования атак на компьютерные сети*.

Были реализованы следующие подзадачи:

- задание структуры атакуемой сети (сетей) с помощью пользовательского интерфейса;
- реализация действий атакующего на микро-уровне;
- введение дополнительной спецификации хостов в атакуемой сети (сетях) для различения типа хоста;
- включение в прототип возможности запуска процесса моделирования атак, когда известна часть данных об атакуемой сети;

Наиболее трудоемкими оказалась реализация двух первых подзадач.

Пользовательский интерфейс для задания структуры сети выполнен в виде wizard. На первом шаге задания атакуемой сети специфицируются все подсети, входящие в структуру атакуемой сети (с использованием понятия *LAN* онтологии *DomainOntology*). Для каждой подсети задается IP-адрес подсети, имя и маска подсети. На втором шаге задания модели атакуемой сети определяются связи между подсетями и месторасположение атакующего по отношению к атакуемой сети. Связи задаются через матрицу смежности. На третьем шаге специфицируются хосты, входящие в каждую из подсетей, и их взаимное расположение на матрице смежности для каждой из подсетей в порядке их задания пользователем на первом шаге. После спецификации всех хостов и всех подсетей вся информация отображается в соответствующие таблицы базы исходных данных атакуемой сети.

Решение подзадачи *реализации действий атакующего на микро-уровне* осуществлено путем задания нескольких классов шаблонов сообщений, объединенных по принадлежности их к тем или иным протоколам передачи данных и типам команд операционной системы. Шаблоны соответствуют заголовкам пакетов в формате тех протоколов, которые задействуются при осуществлении данного конкретного (терминального с точки зрения автоматной модели) действия атакующего. В соответствующих терминальных состояниях автоматной модели выполняется означивание шаблонов необходимыми параметрами. Например, для формирования сообщения на базе шаблона заголовка TCP-пакета получают значения следующие параметры: время, адрес отправителя, адрес получателя, название протокола, значение флага и т.д. По сути дела, реализация действий атакующего на микро-уровне заключается в раскрытии терминальных состояний, в которых осуществляется взаимодействие атакующего с объектом атаки (хостом, сетью, сетями), до уровня, в заданной степени приближенного к реальному выполнению атак на компьютерные сети, – уровня сообщений в рамках используемого протокола передачи данных.

На стороне модели атакуемой сети (хоста) сообщения разбираются с учетом следующей информации:

- специфики объекта атаки – если это хост, то является ли он файеволом или сервером; если это сеть (множество сетей), то присутствуют ли на трассе прохождения атаки хосты, которые могут повлиять на дальнейшее выполнение атаки (здесь в основном имеются в виду файеволы);
- параметров объекта атаки – наличия тех или иных открытых портов, работающих тех или иных приложений, доступности тех или иных ресурсов и т.д.

Ответное сообщение (от модели атакуемой сети (хоста)) формируется с учетом:

- доступности объекта атаки с учетом структуры сети;
- логико-вероятностной модели осуществления данного конкретного действия атакующего;
- степени защищенности объекта атаки (за счет учета модели хоста).

6. *Реализована третья версия программного прототипа системы моделирования атак на компьютерные сети*.

Эта версия программного прототипа системы моделирования атак реализована в виде двух взаимодействующих агентов – агента *MainHack* (агента-хакера) и агента *MainNet* (агента, задающего атакуемую компьютерную сеть).

В основу агента-хакера *MainHack* положена автоматная вероятностная модель переходов от одного атакующего действия к другому. Эта модель является интерпретацией предложенного авторами проекта подхода к генерации атак, основанного на аппарате формальных грамматик. Информационной базой агента-хакера *MainHack* является хранилище информации, полученной от агента *MainNet*.

Агент *MainNet* базируется на вероятностно-атрибутной схеме реакции на действия агента-хакера *MainHack*. В зависимости от конфигурации хоста (сети), запущенных приложений, версий и типов операционной системы, а также от настроек сетевой безопасности агент *MainNet* выдает информацию о сети (хосте) агенту-хакеру в ответ на его сообщение с той или иной вероятностью. Вероятность успеха на стороне агента *MainNet* рассчитывается только в случае удовлетворения всех условий для данного действия хакера, направленного на конкретный атакуемый хост (если целью является один хост) или совокупность хостов (если атака направлена на сеть).

Коммуникация между агентами *MainHack* и *MainNet* в программном прототипе базируется на использовании понятия “Attack” онтологии “Атаки на компьютерные сети”. Всего в текущей версии программного прототипа системы моделирования атак используется 27 атрибутов атаки, в том числе и атрибуты, отражающие результат атак на DNS-сервер.

Приходящие сообщения обрабатываются с использованием соответствующих скриптов. Обработка осуществляется как на стороне агента-хакера *MainHack*, так и на стороне агента *MainNet*. При этом агент-хакер *MainHack* выполняет регистрацию выполненного действия и вычисление последующего действия. После получения входного сообщения (пакета входных сообщений) агент *MainNet* производит его обработку и формирование отклика, направляемого агенту-хакеру.

Для отдельных классов атак (а, следовательно, и сообщений) как на стороне агента-хакера *MainHack*, так и на стороне агента *MainNet* были реализованы специализированные автоматы (с именами “класс/подкласс атаки + _MSG”). Эти автоматы ответственны только за коммуникацию между агентами.

При переходе на двухагентную архитектуру прототипа обработка условий выполнения атакующих действий была исключена из скриптов агента *MainHack*. Она была реализована в отдельной программной компоненте агента *MainNet*. Таким образом, в настоящей версии прототипа при реализации атаки агент-хакер обладает только двумя типами данных об атакуемой сети: (1) спецификация цели атаки; (2) результаты предыдущих атак.

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 представлен один промежуточный отчет (1 июня 2002), в котором представлены соответствующие результаты исследований.

Исполнители проекта совместно с представителями партнера участвовали в семинаре по обсуждению результатов исследований за первый год в феврале 2002 г. в организации партнера в США.

11. Выявленные проблемы и предложения относительно их устранения

Нет

12. Перспективы дальнейшего развития разработанной технологии/научного исследования

Перспективы дальнейшего сотрудничества будут обсуждаться на встрече с представителями Партнера и Министерства обороны США ориентировочно в апреле 2003. Предложения по дальнейшему сотрудничеству были представлены Партнеру в сентябре 2002.

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 №3

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

1. Городецкий В.И., Карсаев О.В, Котенко И.В., Хабалов А.В. Программный инструментарий для разработки и реализации многоагентных систем. // Lecture Notes in Artificial Intelligence, Vol.2296, Springer Verlag, 2002. P.121-130.

   Абстракт. В статье описывается разработанная технология и программное средство для проектирования и реализации основанных на знаниях многоагентных систем. Программное средство включает две компоненты: “Типовой агент” и "Инструментарий разработки многоагентных систем - *Multi-agent System Development Kit*" (MAS DK). Первая компонента включает повторно используемые классы на Visual C++ и Java, а также типовые структуры баз данных и знаний. Вторая компонента содержит несколько ориентированных на пользователя редакторов, служащих для формальной спецификации прикладных многоагентных систем (МАС), находящихся на этапе проектирования и реализации в среде конкретной компьютерной сети. Разработанная технология и MAS DK были использованы при проектировании и реализации прототипов МАС для защиты компьютерных сетей, обнаружения вторжений и моделирования распределенных атак.

2. Городецкий В.И., Котенко И.В. Attacks against Computer Network: Formal Grammar-based Framework and Simulation Tool // A.Wespi, G.Vigna, L.Deri (Eds.). Recent Advances in Intrusion

Detection. Fifth International Symposium. RAID 2002. Zurich, Switzerland. October 2002. Proceedings. Lecture Notes in Computer Science, V.2516. P.219-238.

Абстракт. В статье представлен подход и формальная модель для имитации атак на компьютерную сеть, а также программная реализация имитатора атак на основе использования многоагентной архитектуры. Модель атаки рассматривается как сложный процесс противоборства соперничающих сущностей, а именно злоумышленника или команды злоумышленников, с одной стороны, и системы защиты сети, реализующей определенную политику безопасности, с другой стороны. Статья фокусируется на концептуальном объяснении выбранного подхода, спецификации базовых компонент, составляющих модель атаки, формальных конструкциях для описания указанных компонент и их взаимодействия при выполнении процедуры имитации атак. Особенности разработанного подхода состоят в следующем: (1) моделирование атаки, основанное на учете намерений злоумышленника; (2) многоуровневая спецификация атаки; (3) структурирование модели распределенной атаки, базирующееся на онтологии предметной области; (4) использование атрибутной стохастической *LL(2)* контекстно-свободной грамматики для описания сценариев атаки и их компонент (“простых атак”); (5) использование операции подстановки формальных грамматик для спецификации многоуровневой структуры атак; (6) реализация имитации атак на основе автоматной интерпретации формальных грамматик; (7) генерация действий злоумышленника в реальном времени на основе учета реакции системы защиты атакуемой сети.

3. Городецкий В.И., Котенко И.В. Многоагентные системы для обеспечения безопасности компьютерных сетей // IEEE ICAIS-02. IEEE International Conference “Artificial Intelligence Systems”. Proceedings. IEEE Computer Society. 2002. P.297-302.

Абстракт. В статье рассмотрены приложения многоагентной технологии для проектирования и реализации многоагентных систем (МАС), предназначенные для кооперативного решения критически важных задач в области обеспечения безопасности компьютерных сетей. Эти МАС представлены базирующейся на агентах системой моделирования атак на компьютерные сети, многоагентной системой обнаружения вторжений и многоагентной системой обучения обнаружению вторжений. Каждая из этих МАС базируется на строгом формальном подходе, предложенном авторами, и спроектирована и реализована в виде программного прототипа на основе общей технологии и программного средства “Инструментарий разработки многоагентных систем - Multi-agent System Development Kit”, разработанного авторами работы. В статье проводится обзор указанных МАС, и анализируются преимущества использования многоагентной архитектуры для обеспечения безопасности компьютерных сетей.

4. Городецкий В.И., Котенко И.В. Формальная модель сложных распределенных атак на компьютерные сети // Межрегиональная конференция “Информационная безопасность регионов России”. Материалы конференции. Том 2. СПб, 2002. С.92-97.

Абстракт. В работе рассматривается формальная модель сложных распределенных атак на компьютерные сети. Разработанная формальная модель построена как иерархия контекстно-свободных атрибутных стохастических грамматик, связанных с помощью операции подстановки. Предложенная формальная модель может быть использована в качестве ядра системы, предназначенной для экспериментальной оценки защиты компьютерных сетей, и призвана сыграть важную роль при анализе эффективности используемой политики безопасности.

5. Городецкий В.И., Котенко И.В. Командная работа агентов в антагонистической среде // Международная конференция по мягким вычислениям и измерениям. SMC’2002. Сборник докладов. Том 1. СПб: СПбГЭТУ, 2002. С.259-262.

Абстракт. Агенты формируют команду агентов, если они прилагают совместные усилия для достижения общей цели и функционируют в динамической внешней среде в условиях противодействия противника. В статье рассматриваются вопросы построения команды агентов и организации командной работы в антагонистической среде. Описываются обобщенные модели командной работы. В качестве примера рассматривается реализация предлагаемого подхода для моделирования совместной работы агентов-хакеров.

6. Котенко И.В., Станкевич Л.А. Управления командами автономных объектов в средах с ограничениями времени // IEEE ICAIS-02. IEEE International Conference “Artificial Intelligence Systems”. Proceedings. IEEE Computer Society. 2002. P.121-130.

Абстракт. В работе рассматриваются вопросы управления командами автономных объектов в условиях ограниченного и реального времени. Предложены обобщенные модели командной работы. Представлен общий подход к поддержке командной работы в условиях временных ограничений, базирующийся на комбинировании приближенных вычислений и anytime-алгоритмов. Описаны модели командной работы агентов, реализующие указанный подход для трех различных областей приложений: (1) симуляционного футбола (Robocup), (2) моделирования боевых операций, реализуемых группой автономных летательных аппаратов, (3) имитации распределенных скоординированных компьютерных атак, осуществляемых командой хакеров.

7. Котенко И.В., Маньков Е.В. Моделирование атак на информационно-телекоммуникационные системы // Восьмая Международная Конференция по информационным сетям, системам и технологиям. ICINSAT-2002. Труды. СПб.: СПбГУТ им.Бонч-Бруевича, 2002. С.190-198.

   Абстракт. В работе представлен подход к проектированию и программной реализации системы моделирования программных атак против телекоммуникационных систем. Система моделирования атак предназначена для тестирования безопасности телекоммуникационных систем, уменьшения временных и стоимостных издержек на анализ эффективности механизмов защиты. Система моделирования атак создана на основе онтологии "Моделирование атак на телекоммуникационные системы", формальной модели распределенных атак в виде стохастических атрибутных контекстно-свободных грамматик, ее вычислительной интерпретации с использованием семейства вложенных автоматов, и применения инструментария разработки многоагентных систем MAS DK.

8. Котенко И.В. Многоагентные технологии для обеспечения обнаружения вторжений в компьютерные сети // X Российская научно-техническая конференция (по Северо-западному региону) "Методы и технические средства обеспечения безопасности информации". Тезисы докладов. Санкт-Петербург. Издательство СПбГПУ. 2002. С.44-45.

   Абстракт. В работе представлены основные приложения многоагентных систем в области обнаружения вторжений в компьютерные сети, разработанные в Лаборатории интеллектуальных систем СПИИРАН: (1) агентно-ориентированная система моделирования атак на компьютерные сети; (2) многоагентная система обнаружения вторжений (атак); (3) многоагентная система обучения обнаружению вторжений в компьютерные сети. Каждое из разработанных приложений базируется на предложенных учеными лаборатории формальных моделях и архитектурах и реализовано с использованием собственного инструментария разработки многоагентных систем MAS DK ("Multi-Agent System Development Kit").

9. Городецкий В.И., Котенко И.В. Командная работа агентов-хакеров: применение многоагентной технологии для моделирования распределенных атак на компьютерные сети // КИИ-2002. VIII Национальная конференция по искусственному интеллекту с международным участием. Труды конференции. М.: Физматлит, 2002. С.711-720.

   Абстракт. В работе на примере задачи моделирования скоординированных распределенных атак на компьютерные сети, выполняемых группой агентов-хакеров, рассмотрен подход к реализации командной работы агентов. Подход основан на базовых положениях теории общих намерений и теории разделяемых планов. Предлагаемая технология создания команды агентов включает следующие этапы: (1) формирование онтологии предметной области; (2) определение структуры команды агентов и механизмов взаимодействия и координации; (3) спецификация комплекса планов действий агентов в виде иерархии атрибутных стохастических грамматик; (4) назначение ролей и распределение планов между агентами; (5) автоматная интерпретация сценариев действий команды агентов в процессе ее функционирования. Рассматривается реализация этапов формирования онтологии, спецификации комплекса планов и автоматной интерпретации генерации атак. Описывается прототип многоагентной системы моделирования атак.

10. Котенко И.В. Таксономии атак на компьютерные системы // Труды СПИИРАН, т.3. СПб.: СПИИРАН, 2002.

    Абстракт. В статье представлен обзор таксономий атак на компьютерные системы. Проведен анализ следующих типов таксономий: списки терминов атак; списки категорий атак; категории результатов атак; эмпирические списки; матрицы уязвимостей; таксономии, базирующиеся на действиях; таксономии атак, основанные на их сигнатурах; таксономии дефектов и уязвимостей защиты; таксономии инцидентов.

11. Котенко И.В. Восстановление формальных грамматик, задающих сценарии компьютерных атак, по прецедентам // Искусственный интеллект-2002. Материалы научно-технической конференции. Том.1. Таганрог: Изд-во ТРТУ, 2002.

    Абстракт. В работе анализируются подходы к синтезу формальных грамматик, задающих сценарии атак на компьютерные сети, в том числе: (1) индуктивное восстановление по множеству прецедентов формальными методами; (2) задание экспертом на основе знаний о намерениях злоумышленника и возможных способах реализации этих намерений; (3) комбинирование первого и второго способа. Представлены примеры использования алгоритмов восстановления грамматик, специфицирующих атаки.

12. Котенко И.В. Восстановление формальных грамматик, задающих сценарии компьютерных атак, по прецедентам // Международный научно-теоретический журнал "Искусственный интеллект". № 3, 2002.

    Абстракт. В работе предлагается подход к синтезу (генерации) формальных грамматик, определяющих модели атак на компьютерные сети. Выделено две группы алгоритмов восстановления грамматик: алгоритмы восстановления грамматик перечислением; алгоритмы восстановления грамматик индукцией. В качестве наиболее адекватного выбран метод восстановления регулярной грамматики индукцией по положительному образцу (метод Фельдмана). Дано описание его алгоритмической реализации. Для демонстрации возможностей использования алгоритмов восстановления грамматик, служащих для описания атак на компьютерные сети, рассмотрено несколько прецедентов атак. Представлен пример использования алгоритма восстановления грамматик для спецификации атак на компьютерные сети. Данный подход предлагается использовать при построении многоагентной системы моделирования атак на компьютерные сети.

13. Котенко И.В., Алексеев А.С. Имитация распределенных атак "Отказ в обслуживании" на основе реализации командной работы программных агентов // VIII Санкт-Петербургская Международная Конференция "Региональная информатика-2002" ("РИ-2002"). Материалы конференции. Часть 1. СПб., 2002. С.93-94.

    Абстракт. В работе на примере задачи моделирования распределенных атак "Отказ в обслуживании" (DDoS - Distributed Denial of Service), таких как Trinoo, TFN, Stacheldraht и др., раскрывается предлагаемый подход к организации командной работы программных агентов-хакеров, основанный на использовании парадигмы командной работы группы автономных агентов. Предлагаемая общая технология создания команды агентов, служащая для имитации DDoS-атак, включает следующие этапы: формирование онтологии предметной области моделирования DDoS-атак; определение структуры команды агентов; разработка механизмов взаимодействия и координации агентов; спецификация иерархии планов действий по реализации DDoS-атак; назначение ролей и распределение планов между агентами.

14. Котенко И.В., Степашкин М.В. Классификация атак на Web-сервер // VIII Санкт-Петербургская Международная Конференция "Региональная информатика-2002" ("РИ-2002"). Материалы конференции. Часть 1. СПб., 2002. С.134.

    Абстракт. Предложена классификация атак на Web-сервер по стадиям реализации атаки. Она используется в качестве базиса для описания онтологии предметной области «Атаки на Web-сервер». Атаки на Web-сервер по стадиям реализации разбиваются на группы, обеспечивающие (1) разведку; (2) внедрение; (3) повышение привилегий; (4) реализацию угрозы; (5) сокрытие следов; (6) создание потайных ходов.

15. Котенко И.В., Нестеров С.А. Подход к построению модели источника сетевых атак на базе аппарата формальных грамматик // VIII Санкт-Петербургская Международная Конференция "Региональная информатика-2002" ("РИ-2002"). Материалы конференции. Часть 1. СПб., 2002. С.124-125.

    Абстракт. В работе описывается задача обнаружения неизвестных ранее сетевых атак на компьютерные системы. Рассматривается модель источника сетевых атак на базе математического аппарата формальных грамматик и способы использования данной модели для обнаружения вторжений. Определяется подход к применению разработанной модели для анализа рисков в сфере безопасности компьютерных сетей.

Приложение 4. Информация о патентах и правах на собственность.

Нет

IV. ПОДПИСИ

Руководитель исследований по задаче 1

доктор технических наук профессор
И.В. Котенко