

A

05.13.04

И - 234

ՀՀ գիտութեան համակարգի մշակուած հրատարակուած գիտական աշխատանքի հրատարակում

Իվանյան Էդգար Սևադայի

ՑԱՆՑԱՅԻՆ ՉԱՐԱՇԱՀՈՒՄՆԵՐԻ ԽԱՂԱՅԻՆ և
ԷԲՍՊԵՐՏԱՅԻՆ ՎԵՐԼՈՒԾՈՒԹՅԱՆ ՄԻՋՈՑՆԵՐԻ
ՅԵՏԱԶՈՏՈՒՄ և ՄՇԱԿՈՒՄ և ՆՐԱՆՑ ԻՐԱՎԱՆԱՑՈՒՄԸ
ArmCluster ՅԱՄԱԿԱՐԳՈՒՄ

Ե.13.04 - «Հաշվողական մեքենաների, համալիրների, համակարգերի և
ցանցերի մաթեմատիկական և ժրագրային ապահովում»
մասնագիտությամբ տեխնիկական գիտությունների թեկնածուի
գիտական աստիճանի հայցման ատենախոսության

Ս Ե Ղ Մ Ա Գ Ի Ր

Երևան - 2006

ИНСТИТУТ ПРОБЛЕМ ИНФОРМАТИКИ И
АВТОМАТИЗАЦИИ НАЦИОНАЛЬНОЙ АКАДЕМИИ
НАУК РА

Иванян Эдгар Севадаевич

ИССЛЕДОВАНИЕ И РАЗРАБОТКА СРЕДСТВ ИГРОВОГО И
ЭКСПЕРТНОГО АНАЛИЗА СЕТЕВЫХ ЗЛОУПОТРЕБЛЕНИЙ
И ЕЕ ПРИЛОЖЕНИЕ К СИСТЕМЕ ArmCluster.

А В Т О Р Е Ф Е Р А Т

диссертации на соискание ученой степени
кандидата технических наук по специальности 05.13.04 –
“Математическое и программное обеспечение вычислительных
машин, комплексов, систем и сетей”

Ереван - 2006

Ատենախոսության թեման հաստատվել է Հայաստանի Պետական Երկրաբանական Ռեզերվարատում:

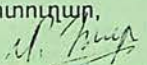
Գիտական ղեկավար՝ ֆ.-մ.գ.դ., պրոֆեսոր Է.Մ.Պողոսյան

Պաշտոնական ընդդիմախոսներ՝ ֆ.-մ.գ.դ., Լ.Հ.Ասլանյան
տ.գ.թ., դոցենտ Գ.Ի.Մարգարով

Առաջատար կազմակերպություն՝ Երևանի Մաթեմատիկական
Մեթոդների Գիտահետազոտական
Ինստիտուտ

Պաշտպանությունը կայանալու է հունիսի «30» 2006 թ. ժամը 15.00` 0014, Երևան քաղաքի Պ. Սևակի 1 հասցեով, ՀՀ ԳԱԱ ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտում գործող 037 «Մաթեմատիկական կիրառական և ինֆորմատիկա» մասնագիտական խորհրդի նիստում:

Ատենախոսությանը կարելի է ծանոթանալ ինստիտուտի գրադարանում:
Սեղմագիրն առաքված է մայիսի « 30 » 2006 թ.

Մասնագիտական խորհրդի գիտական քարտուղար,
ֆ.-մ.գ.թ.,  Ս. Ե. Հարությունյան

Тема диссертации утверждена в Государственном Инженерном Университете Армении.

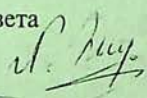
Научный руководитель: д.ф.-м.н., профессор Э.М.Погосян

Официальные оппоненты: д.ф.-м.н., Л.Г.Асланян
к.т.н., доцент Г.И.Маргаров

Ведущая организация: Ереванский Научно-Исследовательский
Институт Математических Машин.

Защита состоится “30” июня 2006 г. в 15.00 часов на заседании Специализированного совета 037 “Математическая кибернетика и информатика” Института проблем информатики и автоматизации НАН РА по адресу: 0014, г. Ереван, ул. П. Севака 1.

С диссертацией можно ознакомиться в библиотеке института.
Автореферат разослан “30” мая 2006 г.

Ученый секретарь специализированного совета
к.ф.-м.н.  М. Е. Арутюнян



25/3-2006

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Создание средств эффективной защиты от вторжений и сетевых атак является одной из первоочередных проблем современных компьютерных систем.

Ключевым компонентом любых средств защиты и областью активных исследований в течении последних десятилетий являются системы обнаружения вторжений (СОВ).

Несмотря на значительные достижения в разработке СОВ полное решение проблемы далеко от завершения. Существующие методы защиты компьютерных сетей, как правило, реализуются в виде набора программных и аппаратных компонент, функционирующих относительно независимо друг от друга, и далеко не безупречно. Системы защиты, имея централизованную структуру, характеризуются неразвитыми адаптационными возможностями, пассивными механизмами обнаружения атак, большим процентом ложных срабатываний при обнаружении вторжений, значительной деградацией трафика целевых информационных потоков из-за большого объема ресурсов, выделяемых на защиту.

С каждым днём к Internet подключаются все больше серверов и их надежная работа становится критически важной. Создаются распределенные сети информационных процессов для обеспечения ученых и инженеров информационными источниками и базами данных высокой эффективности. Целью системы ArgmCluster является создание такой сети для северокавказского региона. Одной из первоочередных задач для сервера ArgmCluster является защита от атак типа “отказ в обслуживании”.

Развитие методов и технологий принятия решений в условиях противодействия с использованием экспертных знаний существенно повышает эффективность систем защиты по сравнению с традиционными методами. Для повышения эффективности исследований по обнаружению уязвимостей методов защиты разрабатываются специальные системы моделирования атак. Настоящая работа выполнена в рамках указанных направлений и имеет следующую цель.

Целью диссертационной работы является построение средств защиты сетей от злоупотреблений и атак, способных в дополнение к существующим системам защиты динамически и с высокой эффективностью вырабатывать на основе игрового анализа и экспертных знаний стратегии защиты, а также интеграция разработанных средств в систему ArgmCluster в среде Linux.

Объекты исследования. Объектами исследования являются системы обнаружения вторжений, игровые модели и методы принятия решений, системы моделирования атак, кластерные и многоагентные системы.

Методы исследования. В диссертационной работе использованы теории программирования игр, статистического анализа, графов, методы объектно-ориентированного программирования.

Научная новизна.

1. Разработана и экспериментально апробирована модель последовательного использования экспертных знаний типа “цели” и “правила” при поиске стратегий в игровом дереве возможных угроз и противодействий. Разработанный на основе этой модели алгоритм IGAF2 (Intermediate Goals At First-2) существенно повышает эффективность защиты компьютерных сетей от вторжений.
2. На основе алгоритма IGAF2 разработана система защиты серверов от сетевых атак.
3. Разработан и экспериментально апробирован инструментарий ИМАМП-2 игрового моделирования атак и методов динамического противодействия
4. Разработана многоагентная система моделирования распределенных атак и оценки методов противодействия.

Практическая ценность и реализация.

Реализована система IGAF2server защиты серверов от сетевых злоупотреблений, а ее Linux версия успешно апробирована в системе ArmCluster.

Система IGAF2server реализована в виде системы программ на языке C++ в среде K Develop 2.0 и Microsoft Visual C++ 6.0 для семейства операционных систем Linux и Windows с ориентацией на объектно-ориентированные технологии.

Система обладает возможностью гибкого изменения и расширения, а также использования в ней как стандартных, так и дополнительных настраиваемых модулей.

Реализован инструментарий моделирования атак и методов противодействия ИМАМП2 в среде Borland C++ Builder 6.0.

Реализована система моделирования распределенных многоагентных атак и обнаружения вторжений в среде ArmCluster, с использованием технологии MPI.

Средства защиты внедрены и используются в системе ArmCluster. ИПИА НАН РА, а также в учебных курсах по защите сетей в Государственном Инженерном Университете Армении с 2006г.

Работа по защите системы ArmCluster выполнена в рамках государственной целевой программы 04.10.31 “Создание государственной научной вычислительной системы РА” в ИПИА НАН РА.

Публикации и апробация. Основные результаты и положения диссертационной работы обсуждались и докладывались на международной научной конференции “Autonomous Intelligent Systems Agents and Data Mining” [Санкт Петербург, Россия, июнь 2005], в Advanced Studies Institute NATO “Multisensor Data and Information Processing for Rapid and Robust Situation and Threat Assessment” [Албена, Болгария, май 2005], на 5-ой международной научной конференции “Computer Science and Information Technologies”, [CSIT2005, 19-23 September, 2005, Yerevan], а также на конференциях и семинарах: в ИПИА НАН РА, на кафедре МОВС ГИУА, на двух научных конференциях в ГИУА [октябрь 2004, 2005].

Научные результаты исследований и основные результаты работы отражены в 6 публикациях, список которых приведен в конце автореферата.

Структура и объем работы. Диссертационная работа состоит из введения, пяти глав, списка использованной литературы и двух приложений. Объем работы - 137 страниц, включая 32 рисунков, 6 таблиц, цитируемую литературу, насчитывающую 110 наименований, и 2 страниц приложений. Диссертация написана на русском языке.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении сформулированы цель и задачи диссертационной работы, обоснована их актуальность, кратко изложены основные результаты работы.

В первой главе проведен анализ работ по СОВ. Описаны существующие технологии принятия решений в задачах слияния данных. Рассмотрена многоагентная технология разработки систем. В §1.1 представлен обзор достижений в области систем обнаружения и противодействия вторжениям. Рассмотрены, в частности, следующие методы обнаружения вторжений:

➤ ***СОВ на основе обнаружения злоупотреблений***, при которых выявляется предопределенная сигнатура - набор событий, однозначно описывающих известное нападение.

Системы на основе сигнатуры заранее запрограммированы на обнаружение известных нападений и генерируют значительно малое число ложных срабатываний. Они эффективны и являются основным средством защиты в коммерческих программах, но должны постоянно модифицироваться сигнатурами новых нападений. “Жесткость” описания сигнатур затрудняет обнаружение ими вариантов традиционных нападений, незначительно отличающихся от базовых.

➤ *СОВ на основе выявления аномалий.* Такие системы обнаруживают нападения, идентифицируя необычное поведение (аномалии) на сервере или в сети. Принцип их функционирования основан на том, что нападающие ведут себя не так, как правомочные пользователи, и могут быть обнаружены системами, идентифицирующими эти различия. Системы на основе выявления аномалий устанавливают базис нормального поведения, профилируя специфических пользователей или сетевые подключения, и выявляют случаи отклонения контролируемой деятельности от нормы. К сожалению, на сегодняшний день системы данного класса пока еще часто производят большое количество ложных срабатываний. Однако, несмотря на это, исследователи утверждают, что они способны обнаружить нападение, ранее незамеченное, в отличие от СОВ на основе сигнатуры, которые полагаются на результаты анализа прошлых нападений. Некоторые коммерческие СОВ реализуют ограниченные формы обнаружения аномалий, однако лишь единицы полагаются исключительно на эту технологию.

В §1.2 представлен обзор работ по технологиям принятия решений в задачах объединения данных, поскольку исследуемые в диссертационной работе данные по защите сетей являются распределенными и гетерогенными, т.е. характеризуются разнообразием физической природы, шкал измерений, структур представления и т.д.

В §1.3 представлен обзор работ по моделированию атак и защиты от сетевых злоупотреблений. Необходимость в моделировании и симуляции атаки появилась с момента появления первых инцидентов проникновения в компьютеры и вычислительные сети. Использование знаний, полученных от обобщения и формализации причин уязвимости компьютерных систем и случаев атак, может значительно улучшить эффективность существующих механизмов защиты.

В §1.4 рассмотрены основные достижения в области разработки многоагентных систем. В настоящее время многоагентная система рассматривается как множество интеллектуальных агентов, распределенных по сети, мигрирующих по ней в поисках релевантных данных, знаний и процедур, и кооперирующихся в процессе выработки решений. Основные достижения в этой области пока мало ориентируются на аспекты практической реализации.

В §1.5 представлен обзор работ по игровым моделям обеспечения оптимальных стратегий. Приведены результаты эффективного использования игровых моделей в менеджменте, системах безопасности и обнаружения вторжений. Рассмотрена корректность и достижимость обеспечения оптимальных стратегий для моделей, описываемых деревом игры. Представлены модели, в которых стратегии получают путем планирования на основе экспертных знаний общего типа и тестирования планов в дереве игры. Практика показала, что игровые модели и методы принятия решений в различных областях по качеству решения задач

планирования и поиска стратегий могут быть сравнимыми и даже превосходить экспертов. Однако проблема систематического повышения эффективности этих моделей и методов на основе экспертных знаний далека от окончательного решения.

В второй главе представлен Инструментарий Моделирования Атак и Динамического Противодействия -2 (ИМАМП2). Описаны требования, предъявленные к инструментарию при его построении. Подробно рассмотрены примеры защиты от атак типа "отказ в обслуживании", SYN-Flood и Fraggle.

В отличие от модели ИМАДП-1, представленной в [Pogossian E. Javadyan A. A Game Model For Effective Counteraction Against Computer Attacks In Intrusion Detection Systems, NATO ASI 2003, Data Fusion for Situation Monitoring, Incident Detection, Alert and Response Management", pp.685-707.], данная модель обладает следующими преимуществами:

- Разработано новое инструментальное средство с использованием технологий VCL и QT для его применения в операционной среде Linux и Windows.
- Разработана новая архитектура для инструментального средства, которое позволяет выбирать подмножества описанных действий и повторно проводить опыт, определяя оптимальные подмножества для защиты от атак.
- Разработана новая архитектура для классификатора состояний, которая позволяет более точно определить состояние системы вовлекая мониторинг различных пакетов сетевого типа, степень занятости центрального процессора, список работающих процессов и степень занятости оперативной памяти.
- Разработана эффективная версия алгоритма минимакс, благодаря которой исключается повторное прохождение по дереву игры и, соответственно, ускоряется поиск наилучшей стратегии. Время, потраченное на построение дерева в случае работы алгоритма минимакс2, на 20% меньше, чем при работе алгоритма минимакс1.

В пункте 2.2.1 дано описание основных структур ИМАМП2 и их функций, а в пункте 2.2.2 рассмотрена архитектура разработанного инструментария (рис. 2.1).

В третьей главе описан метод усечения дерева игры посредством последовательного выделения и достижения подцелей основных целей. По аналогии с алгоритмом Ботвинника определены понятия траектории атаки и зоны противодействия. Представлено описание и блок-схема алгоритма IGAF2 поиска стратегий противодействия.

Эффективность разработанного алгоритма IGAF2 продемонстрирована экспериментами, в которых результаты алгоритма IGAF2 сравниваются с результатами, полученными в ходе экспериментов, проводимых с алгоритмом поиска стратегий по минимаксу и IGAF1.

В пункте 3.1.1 рассмотрены основные структуры, а в пункте 3.1.2 представлена блок-схема алгоритма.

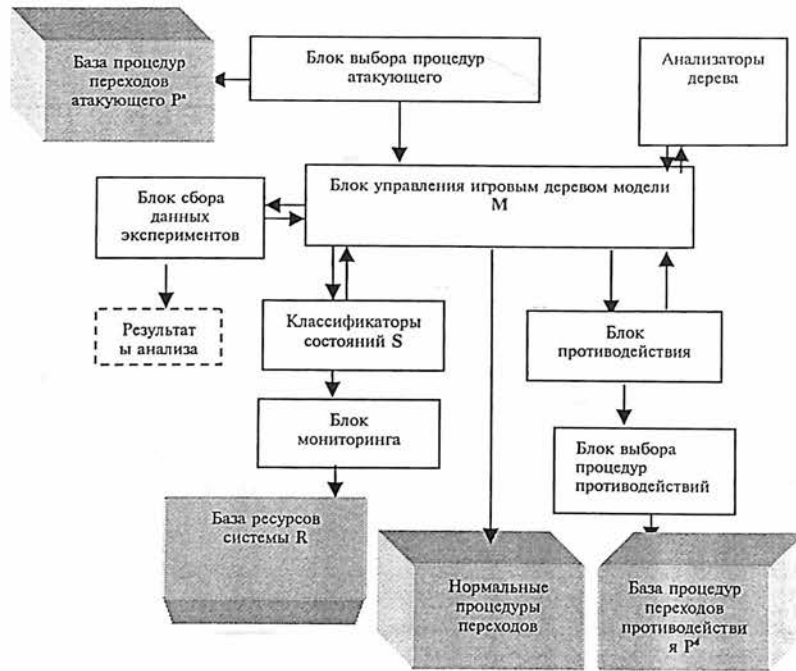


Рис. 2.1. Архитектура инструментария моделирования атак и динамического противодействия.

В данной модели цель алгоритма поиска наилучшей стратегии сводится к решению неточной переборной задачи, решаемой с помощью процедур, аналогичных выделению подцелей по Ботвиннику на усеченном дереве перебора. Соответствующие понятия траектории поражения и зоны противодействия определены следующим образом

- **Траектория поражения**

Траекторией поражения является поддерево $G^a(S', P')$, где

S' - подмножество состояний системы $S' \subseteq S$;

P' - подмножество действий, включающих процедуры переходов атакующего P^a и "нормальные" процедуры переходов противодействующего P^{dH} , т.е. $P' = P^a \cup P^{dH}$, $P' \subseteq P$, $P' \neq \emptyset$.

Надо также отметить, что терминальная вершина графа G^a на глубине $g = N_L$ соответствует критическому состоянию $s'_i \in S$, т.е. $s'_i = 1$.

- **Зона противодействия**

Зоной противодействия является поддерево $G^z(S'', P'')$, построенное вокруг графа траектории поражения $G^a(S', P')$, т.е. $G^z \subseteq G^a$, где S'' - подмножество состояний системы $S'' \subseteq S$, включающее подмножество возможных состояний системы, находящихся на траектории поражения, следовательно $S' \subseteq S''$; а P'' - подмножество действий, включающее процедуры переходов, определенные на траектории поражения P' и процедуры переходов "отражения" противодействующего P^{dO} , т.е. $P'' = P' \cup P^{dO}$, $P'' \subseteq P$, $P'' \neq \emptyset$, следовательно, $P' \subseteq P''$.

В алгоритм IGAF2 включены формальные модели экспертных знаний типа "цели" и "правила", содержательно описываемые следующим образом:

Цели:

1. критические и нормальные состояния определяются дискретизацией значений состояний системы; любое состояние системы со значением соответствующего критерия качества большим или равным некоторому порогу, может быть определено как критическая цель,
2. подозрительные и нормальные ресурсы определяются диапазоном состояний классификаторов ресурсов; комбинации значений классификаторов, интерпретированные как подозрительные или нормальные, индуцируют сигналы для соответствующих действий.

Правила:

1. Опознать подозрительные ресурсы классификаторами и сузить поиск к соответствующему поддереву игры
2. Избегать критических состояний и приближаться к нормальным
3. Нормализовать состояние системы. Сначала, пробовать такие действия защиты, влияние которых на ресурсы вызвало бы изменение его текущего состояния и, если они не помогают, пробовать другие
4. В построении поддерева игры для подозрительных ресурсов использовать:
 - действия защиты, способные влиять на такие ресурсы
 - использовать нормальные действия, пока нет критических состояний
 - если некоторые защитные действия использовались на предыдущих шагах, уменьшить приоритет их использования
5. Уравновесить параметры ресурсов, держа их в диапазонах разрешаемых изменений.

Алгоритм IGAF2 включает следующие этапы работы:

- Число узлов, обработанных алгоритмом IGAF2, со всеми экспертными правилами, и подцелями существенно уменьшается по сравнению с алгоритмом IGAF1 или минимакс.
- Число узлов, обработанных алгоритмом IGAF2, со всеми экспертными правилами и подцелями, является наименьшим по сравнению с алгоритмом IGAF1 или минимакс, когда глубина поиска увеличивается до 13
- Время работы алгоритма IGAF2 со всеми экспертными правилами и подцелями, является наименьшим по сравнению с алгоритмом IGAF1 или минимакс, когда глубина поиска увеличивается до 13.
- Рекомендованная версия алгоритма IGAF2, со всеми экспертными правилами и подцелями, при глубине поиска 5 и при 200 шагах защиты, превосходит "Производительность" - объем полезной работы системы за единицу времени (полезная работа системы, измеренная либо количеством обработанных пакетов, либо допущенных (login) в систему пользователей, либо обработанных файлов и т.д.) минимакс алгоритма на 14%-ов, используя для этого в 6 раз меньше времени вычисления и обрабатывая в 27 раз меньше узлов дерева.

В четвертой главе представлена реализация системы защиты от сетевых злоупотреблений в среде Linux и ее приложение к системе ArmCluster.

В §4.1 описаны особенности защиты системы ArmCluster, сервер которой работает на базе операционной системы Red Hat Linux 9.0 и является основным звеном связи с пользователями (рис. 4.1).

Для сервера ArmCluster первоочередным становится задача защиты от атак "отказ в обслуживании", ибо при неработоспособности сервера весь Cluster теряет работоспособность. Решение задачи защиты сервера ArmCluster нами сведено к решению следующих подзадач:

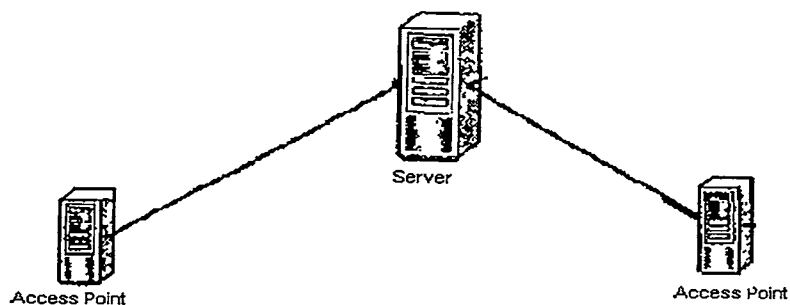


Рис 4.1. Архитектура ArmCluster-a.

1. Разработка блока мониторинга состояний ресурсов сервера
2. Исследование структуры Kernel (Linux)
3. Исследование механизмов обеспечения мониторинга системных ресурсов
4. Реализация механизмов взаимосвязи блока мониторинга с файловой системой "proc - process information pseudo - filesystem"
5. Реализация блока мониторинга
6. Проведение экспериментов для выявления приемлемого интервала времени мониторинга, такого чтобы:
 - не загружать систему лишней работой,
 - иметь адекватную информацию о состоянии системы
 - использовать интервал времени как переменную величину, которая меняется в зависимости от состояния тех ресурсов, над которыми ведется мониторинг
7. Разработка блока оповещения, предназначенного для информирования администратора о критических состояниях ресурсов.

В §4.2 описана архитектура системы TDAS - Threats Dynamic Analysis Software, защиты сервера от вторжений.

В пункте 4.2.1 описаны основные понятия мониторинга ресурсов (рис. 4.2)

4.2) Контролируются следующие ресурсы:

- производительность центрального процессора
- мониторинг сетевых пакетов
- оперативная память
- запоминающее устройство жесткий диск.

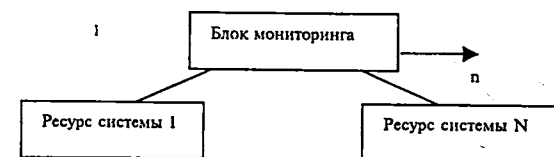


Рис 4.2. Блок мониторинга

Мониторинг сетевых пакетов. Основной целью мониторинга сетевых пакетов является получение информации о таких пакетах, с целью дальнейшего анализа. Мониторинг сетевых пакетов выполняется для выявления потенциальных сетевых атак и их анализа. Учитывая возможные сложности в процессе мониторинга, в частности, обработку большого объема информации за единицу времени, необходимость не перегружать излишней работой систему, была разработана следующая архитектура (рис. 3).

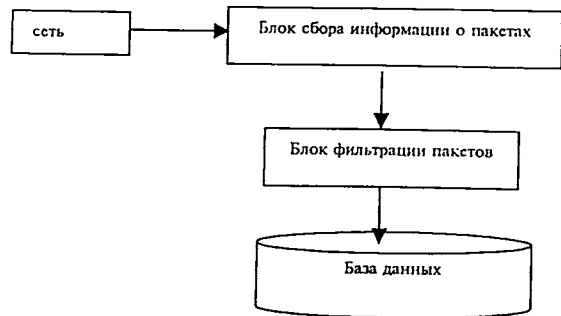


Рис 4.3. Архитектура системы мониторинга сетевых пакетов.

Для дальнейшего анализа используются в частности:

1. Количество открытых соединений.
2. Количество открытых соединений в отдельный период времени.
3. Количество полуоткрытых соединений (соединения в состоянии SYN)

Используя всю эту интегральную информацию, система принятия решений может подвергнуть анализу текущее состояние и, соответственно, принять решение.

Система принятия решений. Система принятия решений анализирует данные полученные из системы мониторинга, выполняет анализ текущей ситуации на основе алгоритмов минимакса или IGAF2 и принятое решение регистрируется в базе решений.

Блок представления опасностей. Блок представления опасностей предоставляет механизмы записи и последующего анализа угроз, аномалий, незакономерностей или злоупотреблений

В пятой главе представлена архитектура разработанного инструментария моделирования распределенных атак.

В §5.1 описан метод моделирования, при которой выбираются две команды агентов в компьютерной сети: команда, которая реализует DDoS нападение и команда защиты. Стартовая цель агентов атаки заключается в определении уязвимости компьютерной сети и системы защиты, следующая цель - выполнение распределенных скоординированных нападений.

Цель команды защиты - в защите сети и ее компонент.

В §5.2 представлена архитектура многоагентной системы моделирования атак на компьютерные сети (рис. 5.1).

Консоль системы - это часть многоагентной системы, звено между оператором-хакером, и остальной частью системы.

Агент -менеджер - отвечает за выполнение указаний, поступивших от консоли.

Агент-исполнитель - отвечает за выполнение самой атаки.

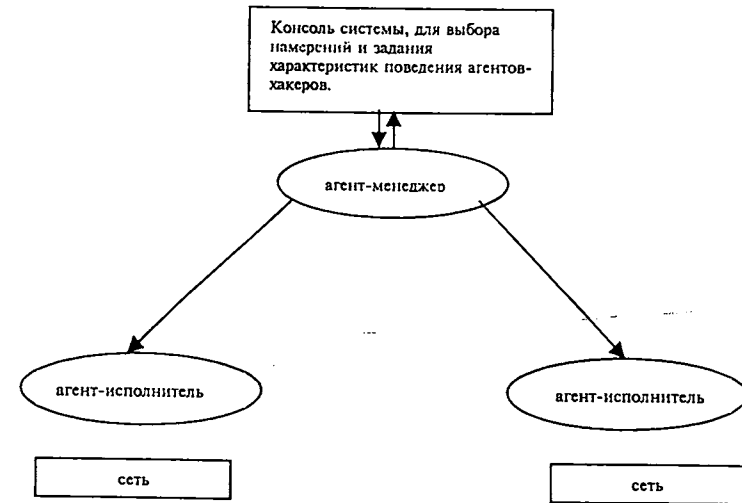


Рис. 5.1. Архитектура многоагентной системы моделирования атак на компьютерные сети.

В §5.3 представлена архитектура многоагентной системы обнаружения вторжений в компьютерные сети. (рис. 5.2).

Агент мониторинга - осуществляет предварительную обработку сообщений.

Фильтр - получает инструкции от агента выполнения решений в виде правил и, в соответствии с ними, осуществляет фильтрацию данных.

Агент классификации - периодически получает информацию от агентов мониторинга и выполняет оценку состояния системы.

Агент принятия решений - отвечает за обнаружение «подозрительных» событий или очевидных фактов вторжения и принятие решений.

Агент выполнения решений - отвечает за выполнение принятых решений, строит правила, которые основаны на командах, полученных от системы принятия решений

В работе представлены основы многоагентной системы моделирования распределенных атак и многоагентные системы обнаружения вторжений в компьютерных сетях.

Представлены архитектура многоагентных систем, типы агентов. Реализуемая система позволит более подробно изучать распределенные атаки, и реализовать более эффективные механизмы защиты.

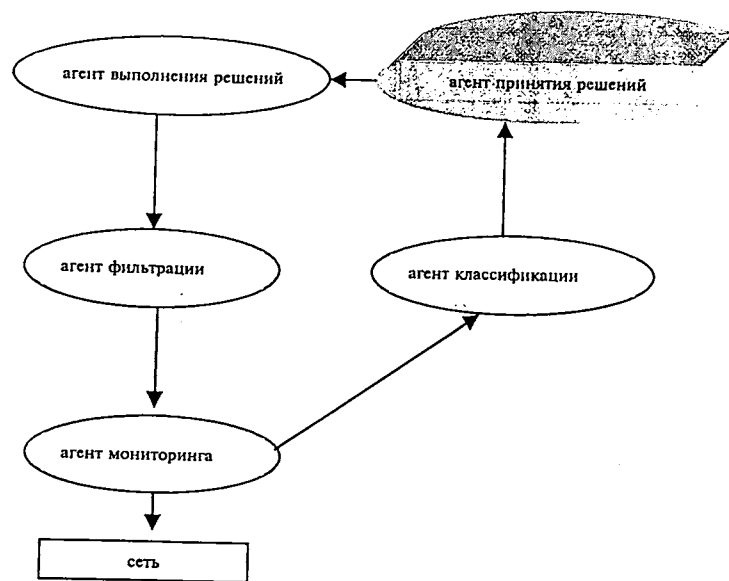


Рис. 5.2. Архитектура многоагентной системы обнаружения вторжений.

В заключении перечислены основные результаты работы.

В приложении 1 приведены справки о внедрении результатов диссертации.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ ДИССЕРТАЦИИ

1. Разработан и экспериментально апробирован алгоритм IGAF2, который при использовании всех экспертных правил и целей существенно повышает эффективность защиты компьютерных сетей от вторжений, а именно, при глубине поиска 5 и при 200 шагах защиты, IGAF2 превосходит "Производительность" минимакс алгоритма на 14%-ов, используя при этом в 6 раз меньше времени вычислений и обрабатывая узлов дерева в 27 раз меньше.
2. Разработана и реализована система IGAF2Linux защиты серверов от сетевых злоупотреблений в среде Linux, на основе динамического анализа возможностей защиты от несанкционированного доступа.
3. На основе IGAF2Linux разработана система TDAS, предназначенная для динамического анализа возможностей защиты от вторжений в сервер ArmCluster-a.
4. Разработан и экспериментально апробирован инструментарий ИМАМП-2 игрового моделирования атак и методов динамического противодействия, обладающий значительными преимуществами по сравнению с моделью ИМАДП-1.
5. Разработана многоагентная система моделирования распределенных атак и оценки методов противодействия, представлены архитектура многоагентных систем, типы агентов и их взаимодействия, а также основы моделирования атак и обнаружения вторжений в компьютерных сетях.

Перечень публикаций по теме диссертационной работы

1. Погосян Э., Джавадян А., Иванян Э., “К построению инструментария моделирования атак и оценки методов противодействия вторжениям”, Научная Конференция ГИУА, Сборник материалов, том 1, С 390-393, Ереван, 2004.
2. Погосян Э., Джавадян А., Иванян Э., “Эксперименты моделирования и оценки методов противодействия при атаках SynFlood и Fraggle”, Вестник Инженерной Академии Армении, том 1, N 3, С 360-368, Ереван, 2004.
3. Pogossian E., Javadyan A., Ivanyan E. “Effective Discovery of Intrusion Protection Strategies”, Autonomous Intelligent Systems, Agents and Data Mining 2005, Lecture Note in Computer Science 3505, pp. 263-274, 2005. ©Springer-Verlag Berlin Heidelberg 2005.
4. Иванян Э., “Адаптация системы IGAF к защите сервера в системе Linux”, Научная Конференция ГИУА, Сборник материалов, том 2, Ереван, С 494-497, 2005.
5. Иванян Э., “Средства динамического анализа угроз злоупотреблений в системе ArmCluster” Computer Science and Information Technologies-2005, Ереван, С 372-376, 2005.

ԱՄՓՈՓՈՒԳԻՐ

Էդգար Իվանյան

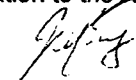
«Ցանցային չարաշահումների խաղային և էքսպերտային վերլուծության միջոցների հետազոտում և մշակում և նրանց իրականացումը ArmCluster համակարգում»

Առենախոսական աշխատության նպատակն է մշակել հարձակումներից և ցանցային չարաշահումները պաշտպանության համակարգ, որը իվիճակի կլինի, ի լրացումն ցանցի պաշտպանվածության ֆիքսված, նախօրոք տրված միջոցների, դինամիկորեն և բարձր արդյունավետությամբ գեներացնել պաշտպանության ստրատեգիաներ՝ խաղային անալիզի և էքսպերտային գիտելիքների հիման վրա և նրանց ինտեգրացումն ArmCluster համակարգում Linux միջավայրում: Ստացվել են հետևյալ հիմնական արդյունքները: -

1. Մշակվել և փորձարարական եղանակով ստուգվել է IGAF2 ալգորիթմը, որն, օգտագործելով էքսպերտային կանոնները և նպատակները, նկատելիորեն բարձրացնում է հարձակումներից կոմպյուտերային ցանցերի պաշտպանության արդյունավետությունը, մասնավորապես, փնտրման 5 խորության և 200 պաշտպանողական քայլերի դեպքում, IGAF2 ալգորիթմը գերազանցում է “արտադրողականությամբ” մինիմալ ալգորիթմին 14 %-ով՝ 6 անգամ քիչ հաշվարկային ժամանակ ծախսելով և 27 անգամ քիչ ծառային զազաթներ մշակելով:
2. Մշակվել և իրականացվել է Linux-ի միջավայրում ցանցային չարաշահումներից սերվերների պաշտպանության IGAF2Linux համակարգը՝ չարտոնագրված ներխուժումներից պաշտպանության հնարավորությունների դինամիկ հակազդեցության հիման վրա:
3. IGAF2Linux համակարգի հիման վրա մշակվել և իրականացվել է TDAS համակարգը՝ նպատակաուղղված ArmCluster-ի սերվերի ներխուժումներից պաշտպանության դինամիկ վերլուծությանը:
4. Մշակվել և փորձարարական եղանակով ստուգվել է ներթափանցումների մոդելավորման և դինամիկ հակազդեցության գործիքային միջոցի երկրորդ տարբերակն՝ առաջին տարբերակի նկատմամբ, բազմակի առավելություններով:
5. Մշակվել է տարածական հարձակումների մոդելավորման և հակազդեցության մեթոդների մշակման բազմաազենտային համակարգը, ներկայացված բազմաազենտային համակարգի ճարտարապետությունը, ազենտների տիպերը և նրանց փոխգործակցությունն, ինչպես նաև, կոմպյուտերային ցանցերում հարձակումների մոդելավորման և ներխուժումների հայտնաբերման հիմքերը:

Edgar Ivanyan

Research and Development Facilities for Expert Knowledge Based Game Tree Analyses of Network Misuses and Their Application to the ArmCluster System



15.05.2014

