УНИВЕРСАЛЬНАЯ СРЕДА ИМИТАЦИИ ПРОЦЕССОВ, ПРОИСХОДЯЩИХ В ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЕ, ОРИЕНТИРОВАННАЯ НА ЗАДАЧИ СИСТЕМ ОБНАРУЖЕНИЯ И ПРОТИВОДЕЙСТВИЯ АТАКАМ

Персиков А.В., Еременко А.С.
Харьковский национальный университет радиоэлектроники
61166 Харьков, пр.Ленина,14, кафедра ТКС, т.702-13-20
E-mail: white_seal@mail.ru, alexere@ukr.net

The given work is handling an actual problem of development of the generic environment for processes simulation that occurred during the network attack performing in the telecommunication system. The widespread simulation environments are analyzed including its facilities and limitations identification, as well as the imperfections that forbid performing an effective intruder and defending sides' actions simulation. The integrated solution that allows consolidating the possibilities of the variety of the environments and forming the common methods library of intrusion detection and prevention system is proposed.

Введение

Важной проблемой в обеспечении информационной безопасности (ИБ) телекоммуникационных систем (ТКС) является создание эффективной системы защиты от кибератак [1]. Опытные злоумышленники способны реализовать продуманные стратегии атак, которые включают [2]:

- сбор информации о ТКС при реализации атаки, идентификацию уязвимостей и защитных механизмов;
- определение путей преодоления защитных механизмов (в том числе, путем моделирования их поведения);
- подавление, нахождение обходных путей, обман компонентов системы защиты, проведение проб уровня защиты незаметным для системы защиты образом или путем проведения распределенных (и разделенных на части) атак с нескольких хостов;
- формирование сложных многофазных атак, присутствие которых сложно определяется подсистемой защиты ТКС;
- получение доступа к ресурсам, повышение привилегий и внедрение несанкционированного кода в отдельных сегментах ТКС для нарушения конфиденциальности, целостности, доступности в сети в целом;
- скрытие внешних признаков атаки.

Реализация мер противодействия атакам выполняется с помощью системы обнаружения и противодействия атакам (intrusion detection and prevention system, IDPS), которая является многокомпонентной распределенной системой, включающей следующие физические компоненты [2]:

- сенсоры, предназначенные для сбора разнотипной информации;
- защищенные каналы для обмена информацией;
- распределенные компоненты обработки информации;
- единый центр или распределенные компоненты принятия и исполнения решения.

IDPS должна поддерживать работу в режиме реального времени для проведения следующих операций:

- реализации механизмов защиты, соответствующих политике безопасности;
- определения вторжения и предсказания намерений и действий злоумышленника;
- оценки потенциальных уязвимостей, сбора данных и анализа текущего состояния сети и системы защиты;
- проведения ответных действий, включая подавление действий злоумышленника и перераспределение нагрузки между критически важными защитными механизмами;

– уменьшения последствий вторжения и определения уязвимостей, адаптации системы ИБ для лучшего противодействия уже изученным атакам в будущем.

Организация защиты от атак с помощью IDPS строится по следующей схеме:

– воспроизведение ситуации в сети в определенной среде имитации процессов, происходящих в ТКС;
– оценка возможных действий злоумышленника относительно сетевых приложений, элементов и протоколов;
– выявление способов противодействия или направления действий злоумышленника и их документирование с помощью определенного языка программирования;
– инсталляция кода (сценария) нового способа противодействия в базе знаний IDPS.

Именно возможности среды имитации определяют качество нового способа противодействия и увеличения функциональных возможностей IDPS, что естественным образом приведет к улучшению показателей распознаваемости атак. Существующие на сегодняшний день среды имитации обладают своими уникальными возможностями, позволяющими реализовать тот или иной функционал, а также присущими им ограничениями и недостатками. Поэтому задачей работы видится анализ возможностей популярных сред имитации, формирование их рейтинга, а также выдвижение предложений по интеграции их возможностей в рамках единой среды имитации.

1 Обзор сред симуляции систем обнаружения и противодействия атакам

Наиболее популярными средами имитации, обладающими развитыми функциональными способностями, являются NetSim (http://www.nsnam.org/), OMNeT INET Framework (http://www.omnetpp.org/), J-Sim (http://www.j-sim.zcu.cz/), SSF Net (http://www.ssfnet.org/), GTNetS (http://www.ece.gatech.edu/). Функциональные возможности сред представлены в табл. 1.

Таблица 1 – Функциональные возможности сред имитации

Возможность	NetSim	OMNeT	J-Sim	SSF Net	GTNetS
Тип симуляции	время	события	время	события	события
Распределенные вычисления	да	да	нет	нет	да
Основной язык программирования	TCL	Eclipse/ C++	Java	Java, C++	C++
Многоплатформенность	эмулятор	да	java	да	да
Сопряжение с реальным оборудованием	да	нет	нет	нет	нет
Модификация коммуникационной платформы	да	да	нет	нет	нет
Протокольный инжиниринг	нет	нет	нет	нет	нет
Программирование агентов взаимодействия	нет	нет	нет	нет	нет
Определение топологических и функциональных компонентов	да	да	нет	да	да
Розыгрыш соревновательной ситуации между злоумышленником и защищающейся стороной	нет	нет	нет	нет	нет
Поддержка IDMEF [RFC 4765], IDXP [RFC 4767] и протоколов-сателлитов	огранич.	нет	нет	нет	нет

Под протокольным инжинирингом понимается возможность формирования сценария взаимодействия сетевых элементов по накопленным сетевым данным и статистике.

Рассмотрение возможностей сред имитации позволил выявить ряд недостатков, критических для проведения анализа сетевых атак:

- отсутствие возможности розыгрыша случайных ситуаций в сети (фиксированная топология сети и размещение сетевых элементов);
- сложность описания состояния сети при проведении множества атак различного вида или многофазовых распределенных атак;
- отсутствие поддержки функций совмещения действия (кооперации) сетевых элементов и программирования агентов взаимодействия, ответственных за координацию действий сетевых элементов (как для атакующей, так и для защищающейся стороны);
- ограниченность взаимодействия сред имитации (лишь на уровне поддерживаемых форматов данных, да и то не во всех случаях);
- поддержка мультиплатформенности за счет эмуляции платформы, что значительно снижает скорость и эффективность имитации (как правило, эмулятор платформы не позволяет задействовать средства распределенных вычислений, поддерживаемые имитатором).

В общем можно определить, что рассмотренные среды изначально не предназначены для анализа параметров сети в состоянии проведения атак и должны быть дополнены определенным интегрирующим элементы, который позволит формировать программные компоненты и накапливать знания относительно задач IDPS.

2 Построение универсальной среды имитации

Создание и отладка полноценной среды имитации «с нуля» является сложной задачей, что приводит к решению о том, что среда должна быть посредником между различными уже существующими средами имитации и библиотеками шаблонов сетевого взаимодействия (рис. 1).

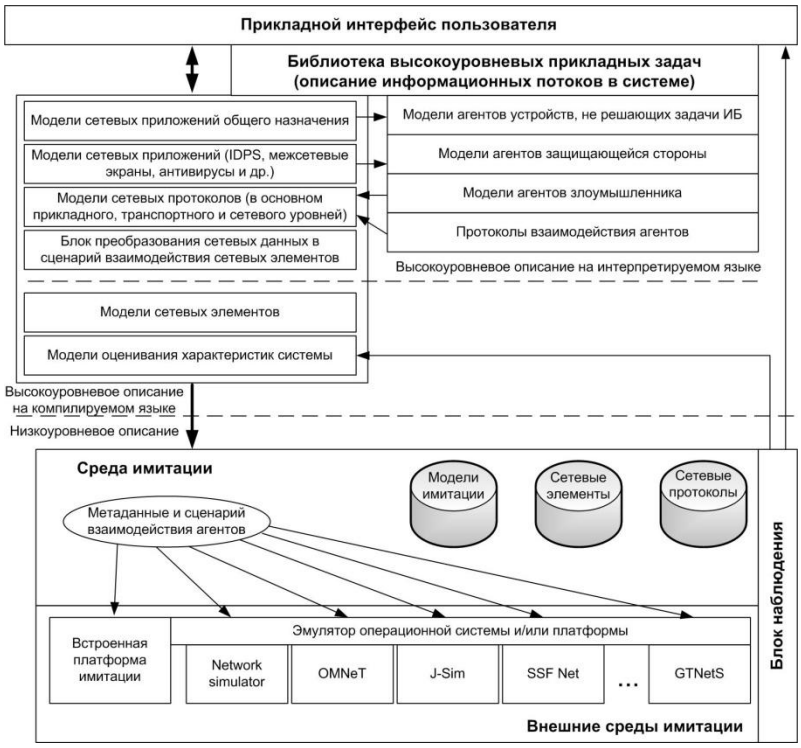

Рис. 1 – Структура среды имитации

Основной идеей универсальной среды имитации процессов (рис. 1) является применение специальной системы интерпретируемых команд, которая преобразуется в специфический для среды имитации и используемой программно-аппаратной платформы набор инструкций (на основе кросс-платформенных языков программирования, таких как C# или Java [3]). Ядром среды является множество моделей: сетевых элементов, протоколов и приложений, информация о которых может быть помещена в общую базу знаний с помощью UML-моделей и моделей конечных автоматов, предоставляемых разработчиками. Большинство современных сред разработки, такие как Visual Studio, Microsoft Visio и другие, позволяют генерировать шаблоны кода на основе диаграмм, формируя библиотеку компонентов на основе кросс-платформенного кода. Используя возможности программного обеспечения промежуточного уровня, такого как CORBA, J2EE, .NET Framework и других, становится возможным проведение прозрачных для разработчика распределенных вычислений и удаленной активации частей среды имитации. Применение агентных архитектур позволяет организовать ролевое управление задачами в имитаторе и логически связать телекоммуникационные процессы и действия атакующей и защищающейся стороны.

Недостатком такого решения является необходимость взаимодействия различных компонентов среды имитации (например, встроенной платформы симулирования и внешних средств имитации) с помощью компонентов-посредников, реализующих интерфейсы взаимодействия, что уменьшает скорость проведения имитации. Такое ограничение частично снимается за счет использования компилируемых языков программирования, поддерживаемых множеством платформ.

Выводы

На основе вышеперечисленного можно сделать вывод, что IDPS является системой с множеством сложных задач и проблем, требующих исследования связей между злоумышленником и подсистемой защиты ТКС. Возможности злоумышленника по проведению атак опираются на возможность анализа информационных потоков и эффективных манипуляций данными на сетевом уровне.

Моделирование и имитация процессов, которые происходят в ТКС во время проведения атак, являются сложными задачами, требующей инструментария с развитыми возможностями. Различные среды имитации предоставляют широкие возможности, однако они ориентированы на решение общесетевых задач и не предназначены для моделирования поведения сетевых элементов, которые управляются атакующей и защищающейся сторонами. Разработка универсальной среды моделирования атак и защитных действий позволит создать общую библиотеку сетевых элементов, протоколов и приложений, использовать распределенные вычисления с применением интерпретируемых языков программирования и сред моделирования параллельных процессов. Связывая среды, ориентированные на «чистое» математическое моделирование (OMNeT, J-Sim и др.) со средами, допускающими использование реального оборудования и высокую распараллеливаемость процесса имитации (например, NetSim), становится возможным масштабирование задачи анализа и управление оборудованием из программ, которые ранее этого не позволяли.

Литература:

1. Kotenko I. Agent-based modelling and simulation of network cyber-attacks and cooperative defence mechanisms. Discrete Event Simulations. Sciyo, In-teh. 2010. P.223-246.
2. Поповский В.В. Защита информации в телекоммуникационных системах. В 2-х т. [Текст] / В.В. Поповский, А.В. Персиков. - Х.: СМИТ, 2006.
3. Troelsen A. Pro C# 2010 and the .NET 4 Platform. – NY.: Apress, 2010. – 1753 p.