УДК 004.056.5

РАЗРАБОТКА АППАРАТНО-ПРОГРАММНОГО КОМПЛЕКСА ДЛЯ РЕАЛИЗАЦИИ ЗАЩИТЫ ВЫЧИСЛИТЕЛЬНОГО АЛГОРИТМА НА ОСНОВЕ МИКРОПРОЦЕССОРНОЙ СИСТЕМЫ

К.И. Костромитин

В статье представлены аспекты разработки аппаратно-программного комплекса для реализации защиты вычислительного алгоритма на уровне отдельных узлов, соединённых в вычислительную сеть на основе древовидной и конвейерной топологий.

Ключевые слова: аппаратно-программная защита информации, топология сети, локализация вычислительных алгоритмов

Актуальность исследования

Актуальность исследований в области защиты информации связана с интенсивной компьютеризацией различных сторон жизни общества и необходимости предотвращения несанкционированного доступа к ним.

Мировые расходы на обеспечение информационной безопасности (ИБ) на текущее состояние: расходы в сферы ИБ на сегодня составляют $81,7 млрд. Прогноз расходов к 2020 году: около $105 млрд [1].

Уязвимости аппаратного характера могут иметь различную природу, например, нарушение работы генератора псевдослучайных чисел, ошибки киптоалгоритмов, конфигурирования системы (начальные параметры), программного обеспечения [1].

Программы, непосредственно предназначенные для выполнения деструктивных действий на атакуемом объекте, являются эксплойтами [2, 3].

Также среди программных методов защиты следует отметить сигнатурный, эвристический анализ, методы внесения неопределённости в работу объектов, контроль хода выполнения программ, использование межсетевых экранов и систем обнаружения вторжений, мониторинг потенциально опасных действий [4, 5].

Текущее состояние проблемы и предполагаемый уровень угрозы

В настоящее время работа вычислительных систем критически важных объектов происходит без доступа к внешней сети для обеспечения требований ИБ.

Предполагаемый уровень угрозы: в рамках представляемой разработки предполагается, что программный уровень защиты информации является принципиально недостаточным для обеспечения стабильного функционирования критически важных объектов ввиду возможной реализации аппаратных уязвимостей вычислительной системы непосредственно на этапе её проектирования и производства.

Наиболее существенными угрозами информационной безопасности с точки зрения защиты алгоритма, функционирующего в вычислительной системе, являются:

1. Возможности аппаратной реализации недокументированных инструкций в различных компонентах вычислительной системы, а также перепрограммирование микрокода – в первую очередь, микропроцессора, жесткого диска и usb-портов.

2. Получение удалённого доступа к вычислительной системе минуя средства программной защиты на аппаратном уровне (например, с целью получение дампа оперативной памяти для проведения дальнейшего анализа).

Одним из вариантов решения проблемы защиты информации в приведённом случае может являться разработка аппаратно-программного комплекса на основе нескольких микропроцессорных систем, обеспечивающего максимально возможную степень защиты произвольного вычислительного алгоритма.

Для достижения поставленной цели может быть сформулировано несколько возможных решений:

1) реализация обмена данными в локальной сети на основе технологии веб-сервера (Apache HTTP-сервер);

2) разработка ПО на основе web-технологий (php) для реализации обмена данных между вычислительными узлами;

3) разработка ПО на основе ЯП C#/C++ для реализации обмена данными между вычислительными узлами.

Описанные решение планируется реализовать на двух топологиях сети: древовидной (рис. 1) и конвейерной (рис. 2).

В случае древовидной топологии вычислительный алгоритм разбивается по узлам и каждый из них проводит независимую обработку поступающих данных, после чего они пересылаются шлюз, через который попадают во внешнюю сеть. В случае конвейерной архитектуры сети каждый узел выполняет часть операций по обработке поступающих данных, после чего следующий узел продолжает выполнение следующей части операций.

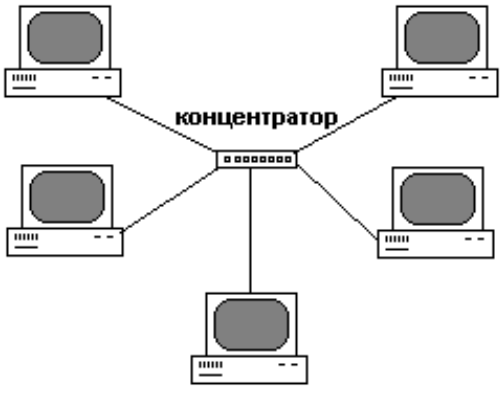

Рис. 1. Древовидная топология соединения вычислительных узлов в локальной сети, роль концентратора играет шлюз

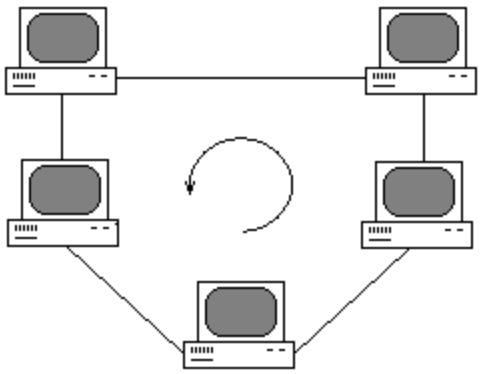

Рис. 2. Кольцевая топология соединения
вычислительных узлов в локальной сети,
роль шлюза может играть произвольный вычислительный узел

Теоретически достижимый уровень защиты вычислительных алгоритмов

Вследствие того, что сложность анализа систем вычислительных устройств является крайне высокой (в первую очередь, CPU) и их работа не является строго контролируемой, максимальный возможный уровень защиты алгоритмов может быть достигнут при применении аппаратных методов изолирования вычислительной системы в локальную сеть за шлюзом с физическим распараллеливанием вычислительной задачи.

Более фундаментального подхода для решения поставленной задачи в настоящее время не выявлено, что дает основания полагать, что реализация предложенных топологий обеспечит максимально возможный уровень защиты вычислительных алгоритмов с точки зрения вопросов аппаратной защиты.

В качестве дополнительных мер защиты системы может быть использовано: реализация виртуальной вычислительной машины и применение аппаратной системы блокирования запросов, поступающих на шлюз со сторонних IP-адресов.

Библиографический список

1. Anderson R. Why Cryptosystems fail, ACM Conférence on Computer and Communication Security, 1993.

2. Щербаков, А. Разрушающие программные воздействия / А. Щербаков. – М.: Издательство Эдэль, 1993. – 64 с.

3. Гриняев, С.Н. Поле битвы киберпространство: теория, приёмы, средства, методы и системы ведения информационной войны / С.Н. Гриняев. – М., 2004.

4. Erickson J. Hacking: The Art of Exploitation. Second Edition: No Starch Press, 2010.

5. Разрушающие программные воздействия: Учебно-методическое пособие / Н.П. Васильев, Е.В. Вельмякина, Д.В. Гуров и др.; под ред. М.А. Иванова. – М.: НИЯУ МИФИ, 2011.

К содержанию