УДК 004.274:004.056

С.Я. Гильгурт, г. Киев

ОРГАНИЗАЦИЯ ВЫЧИСЛИТЕЛЬНОГО ПРОЦЕССА СИНТЕЗА ФАЙЛОВ КОНФИГУРАЦИЙ ДЛЯ АППАРАТНЫХ УСКОРИТЕЛЕЙ ПРИ РЕШЕНИИ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ[1]

Abstract. Methods to synthesize bitstreams for the reconfigurable accelerators aimed to solve computer security tasks are investigated. Using Grid, cloud computing or datacenters as a platform for organizing a remote centralized service for this purpose is proposed.

Введение

Прекращение роста частоты микропроцессорных систем вследствие технологического предела в производстве микроэлектроники способствовало повышению интереса к аппаратным решениям. Основное внимание уделяется, как правило, реконфигурируемым устройствам на базе программируемых логических интегральных схем (ПЛИС), которые обладают гибкостью, сопоставимой с программными решениями, сохраняя быстродействие специализированных аппаратных схем [1].

Одной из областей применения аппаратных ускорителей, где использование программируемой логики получает широкое распространение в последние годы, является информационная безопасность. Постоянно растущие объемы информации, которая хранится, передается и обрабатывается в компьютерных системах, а также повышение интенсивности и изощренности вредоносной активности приводит к тому, что традиционные микропроцессорные решения не справляются с повышением вычислительной нагрузки.

Наиболее злободневны данные проблемы при создании систем обнаружения / предупреждения вторжений (СОВ / СПВ), антивирусных средств, систем контроля целостности и других технических средств, предназначенных для решения задач информационной безопасности [2].

Анализ последних исследований и публикаций показывает, что процесс разработки и конфигурирования аппаратного устройства на базе ПЛИС является сложной и ресурсоемкой задачей, требующей, с одной стороны, интеллектуального труда квалифицированных специалистов, с другой – значительных вычислительных затрат.

Пользователи систем информационной безопасности (системные администраторы) как правило, не имеют возможностей для самостоятельной разработки аппаратных СОВ и антивирусных систем. С другой стороны,

[1] Исследование выполнено при частичном финансировании по Целевой комплексной программе научных исследований НАН Украины «Грид-инфраструктура и грид-технологии для научных и научно-прикладных применений», 2015 г.

использование готовых разработок сторонних производителей не представляется возможным в силу разнообразия и ярко выраженной переменчивости параметров операционной среды информационной безопасности, в которой функционируют защищаемые компьютерные системы.

Целью настоящей работы является исследование возможности организовать вычислительный процесс синтеза реконфигурируемых средств информационной безопасности таким образом, чтобы сложные и ресурсоемкие процедуры выполнялись не локально на каждой отдельной системе, а централизовано, с применением высокопроизводительных компьютерных систем.

1. Принципы построения реконфигурируемых средств информационной защиты

Исторически первыми и, как следствие, наиболее исследованными средствами информационной защиты, использующими преимущества программируемой логики, явились сетевые системы обнаружения вторжений (ССОВ), соответствующий англоязычный термин – Network Intrusion Detection System (NIDS). Применение ПЛИС позволило эффективно преодолеть главную проблему, возникающую при защите локальных сетей от внешних атак, связанную с высокой вычислительной ресурсоемкостью операции распознавания сигнатур в интенсивном потоке сетевых пакетов.

В работе [3] был проведен анализ возможностей ПЛИС и способов ее применения в составе СОВ. В частности, указано, что аппаратные решения на базе программируемой логики применяются, главным образом, в СОВ на основе сигнатур (Signature-based IDS). Наиболее ресурсоемким этапом обработки информации в таких системах является процедура распознавания образцов (pattern matching), которая сводится к выполнению большого количества операций сравнения содержимого сетевых пакетов с последовательностями символов из базы данных сигнатур.

По этой причине наиболее важным компонентом ССОВ, от успешной реализации которого во многом зависит эффективность системы в целом, является модуль распознавания сигнатур. В работе [4] рассмотрена обобщенная структура СОВ на базе ПЛИС.

В работе [5] исследованы подходы к построению аппаратного модуля распознавания на базе программируемой логики. На сегодняшний день для этой цели успешно применяются такие подходы и технические решения, как:

- цифровые автоматы;
- устройства ассоциативной памяти и ее разновидности;
- схемы на базе хэш-функций, в частности, фильтр Блума,

а также их комбинации.

В результате реализации любого из перечисленных выше подходов набор сигнатур, подлежащих распознаванию, оказывается "прошитым" в вычислительной структуре модуля распознавания на аппаратном уровне.

Базы данных сигнатур современных СОВ содержат большое число

символьных образцов. Синтез аппаратной схемы для их одновременного распознавания невозможно выполнить вручную. Для автоматизации данного процесса разрабатываются специальные программные средства, позволяющие по имеющемуся набору правил генерировать описание реализуемой структуры на каком-либо языке описания аппаратуры, например, VHDL. В работе [4] описана обобщенная структура процесса автоматизированной генерации конфигураций, загружаемых в ПЛИС сетевой СОВ.

2. Проблемы синтеза файлов конфигураций для аппаратных ускорителей при решении задач информационной безопасности

Рассмотрим сложности, которые возникают при создании и эксплуатации реконфигурируемых средств аппаратного ускорения для задач информационной безопасности.

2.1. Общие сложности синтеза конфигураций для ПЛИС. Одним из основных недостатков реконфигурируемых вычислителей является сложность создания конфигураций – последовательностей битов (bitstream), загружаемых в микросхему ПЛИС для придания ей требуемой функциональности. Процесс создания конфигураций помимо собственно разработки цифровой схемы, решающей поставленную задачу, включает в себя ряд вычислительно емких процедур, таких как синтез (Synthesize), трансляция (Translate), отображение (Map), размещение и трассировка (Place & Route), генерация файла конфигурации (Bitstream Generating). Эти процедуры выполняются без участия разработчика с использованием либо фирменного пакета САПР от производителя ПЛИС, либо специализированного программного обеспечения, например, системы автоматического синтеза конфигураций для СОВ. В случаях, когда синтезируются сложные схемы, использующие по максимуму ресурсы старших моделей современных ПЛИС (содержащих миллионы эквивалентных логических элементов), процедура синтеза может занимать по времени от десятков минут до нескольких часов.

2.2. Специфика использования реконфигурируемых средств защиты информации. Угрозы информационной безопасности в компьютерных системах характеризуются высокой степенью динамичности, которая обусловлена стабильно нарастающей активностью злоумышленников. Так, в современных системах антивирусной защиты обновление баз данных сигнатур, вызванное появлением новых вредоносных программ, осуществляется в среднем несколько раз в сутки.

С другой стороны, для деятельности по защите информации в компьютерных системах характерно разнообразие многочисленных настроек и режимов работы программного обеспечения, что делает каждый защищаемый объект (компьютер, локальную либо корпоративную сеть) уникальным, не похожим на другие. Так, база данных сигнатур наиболее популярной из свободно распространяемых систем обнаружения вторжений Snort [6] содержит несколько десятков тысяч правил, любое из которых

системный администратор – пользователь СОВ может включить либо выключить в зависимости от назначения и свойств защищаемого объекта.

Как указывалось выше, при синтезе вычислительной структуры блока распознавания СОВ сигнатуры "прошиваются" на аппаратном уровне. Следовательно, каждому пользователю в общем случае требуется своя собственная, уникальная конфигурация для ПЛИС ускорителя. И эту конфигурацию необходимо синтезировать заново как при изменении настроек СОВ, так и при добавлении в базу данных сигнатур вновь обнаруженных атак, распространяющихся на данный объект.

3. Предлагаемое решение

Резюмируя рассмотренные выше проблемы синтеза конфигураций для аппаратных ускорителей задач информационной безопасности, можно сформулировать научно-техническую задачу в следующей постановке.

Имеется большое число объектов обработки информации (различных как по масштабу, так и по присутствующим рискам), для защиты которых используются реконфигурируемые устройства информационной безопасности, функционирующие по схожим алгоритмам, но построенные в общем случае на базе ПЛИС разных типов различной вычислительной мощности. Вследствие частого изменения условий функционирования защищаемых объектов (с частотой от нескольких часов до нескольких суток) требуется оперативное реконфигурирование ПЛИС. В техническом смысле данное требование сводится к выполнению однотипных процедур, ресурсоемких в вычислительном смысле, но не требующих вмешательства человека. При этом пользователи устройств информационной безопасности (системные администраторы объектов) не обладают ни навыками организации процесса синтеза необходимых конфигураций, ни достаточными вычислительными ресурсами.

Исходя из такой постановки, логично предложить использование централизованной системы, работа которой была бы организована в виде удаленного сервиса и включала в себя выполнение следующих функций.

1) сбор исходных данных о текущих параметрах безопасности с каждого из объектов, с одной стороны, а также оперативное пополнение имеющихся баз сигнатур актуальной информацией о вновь обнаруженных факторах злонамеренной активности (атаках, вирусах и т.п.) – с другой;

2) формирование и поддержка в актуальном состоянии перечня конфигураций, необходимых для удовлетворения потребности всех клиентов, с учетом как настроек безопасности для каждого из защищаемых объектов, так и параметров ПЛИС в соответствующих аппаратных ускорителях;

3) максимально быстрая генерация файлов конфигураций согласно упомянутому выше перечню;

4) оперативная доставка конфигураций потребителям.

Заметим, что со стороны потребителя данный сервис выглядит аналогично механизму централизованной рассылки обновлений в широко

распространенных антивирусных системах. Отличие лишь в том, что файлы коррекции антивирусной базы заменяются файлами загружаемых в ПЛИС конфигураций.

В качестве платформы для реализации предлагаемого сервиса могут выступать известные высокопроизводительные и / или распределенные компьютерные технологии, в частности, грид-сети, облачные вычисления, центры обработки данных и т.п.

Выводы

В настоящей работе предложена идея эффективного способа организации вычислительного процесса синтеза конфигурационных последовательностей для ПЛИС, входящих в состав реконфигурируемых аппаратных ускорителей, применяемых для решения задач информационной безопасности.

В структурном плане вычислительный процесс включает в себя на нижнем уровне набор реконфигурируемых устройств, обеспечивающих информационную защиту компьютерных объектов, а на верхнем – удаленный централизованный сервис, организованный на базе одной из современных высокопроизводительных (распределенных) компьютерных технологий.

Пользователи системы (системные администраторы либо иные лица, ответственные за информационную безопасность) через соответствующий интерфейс передают сервису нужные данные (списки сигнатур, подлежащих распознаванию, параметры СОВ и т.п.), а получают результаты обработки в виде конфигураций – двоичных файлов для программирования ПЛИС.

1. *Гильгурт С.Я.* Реконфигурируемые вычислители. Аналитический обзор // Электронное моделирование. – 2013. – Т.35, № 4. – С. 49–72.
2. *Hilhurt S. Ya.* Application of FPGA-based Reconfigurable Accelerators for Network Security Tasks // Collection of scientific works. Simulation and informational technologies. – PIMEE NAS of Ukraine. – Kyiv, 2014. – Vol. 73. – P. 17–26.
3. *Гильгурт С.Я.* Анализ применения реконфигурируемых устройств в системах обнаружения вторжений // Тез. доп. Міжнар. наук.-техн. конф. «Моделювання-2010». Т.1. – Київ: Інститут проблем моделювання в енергетиці ім. Г.Є.Пухова НАН України, 2010. – С. 260–267.
4. *Коростиль Ю.М., Гильгурт С.Я.* Принципы построения сетевых систем обнаружения вторжений на базе ПЛИС // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ НАН України. – Київ, 2010. – Вип. 57. – С. 87–94.
5. *Давиденко А.Н, Гильгурт С.Я.* Алгоритмы распознавания строк в системах обнаружения вторжений на ПЛИС // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ НАН України. – Київ, 2010. – Вип. 58. – С. 103–109.
6. *Давиденко А.Н., Гильгурт С.Я., Сабат В.И.* Аппаратное ускорение алгоритмов сигнатурного обнаружения вторжений в открытой системе информационной безопасности Snort // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ НАН України. – Київ, 2012. – Вип. 65. – С. 94–103.

Поступила 7.9.2015р.