УДК 004.274:004.056

Ю.М. Коростиль, д-р техн. наук, ИПМЭ им. Г.Е. Пухова НАНУ, г. Киев
С.Я. Гильгурт, канд. техн.наук, ИПМЭ им. Г.Е. Пухова НАНУ, г. Киев

ПРИНЦИПЫ ПОСТРОЕНИЯ СЕТЕВЫХ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ НА БАЗЕ ПЛИС

The common principles of FPGA-based NIDS (Network Intrusion Detection Systems) construction are investigated. The main requirements and characteristics of such systems are discussed. The generalized structure of a reconfigurable NIDS is described.

Сетевые системы обнаружения вторжений (ССОВ), соответствующий англоязычный термин – Network Intrusion Detection System (NIDS), являются важным инструментом информационной безопасности, все более широко используемым для защиты локальных вычислительных сетей от воздействия внешних вредоносных факторов. В связи с постоянным ростом числа и сложности компьютерных атак, а также из-за значительного увеличения объемов данных, передаваемых в сети, традиционные программные решения все хуже справляются с поставленными задачами. Ситуация усугубляется технологическим пределом, достигнутым недавно в микроэлектронной промышленности, в результате которого неизменный на протяжении десятилетий рост частоты микропроцессоров остановился.

Этими причинами обусловлен повышенный интерес к использованию в качестве аппаратной основы ССОВ программируемых интегральных схем (ПЛИС) типа Field Programmable Gate Array (FPGA) [1].

В настоящей статье рассмотрены основные принципы построения сетевых систем обнаружения вторжений с применением программируемой логики.

Анализ информационных источников свидетельствует о наличии большого количества англоязычных публикаций по применению реконфигурируемых устройств на базе FPGA в составе NIDS. В то же время, информация на данную тему, фактически, отсутствует в литературе, издаваемой в странах СНГ.

Целью настоящей работы является исследование и обобщение основных принципов построения систем обнаружения вторжений на базе программируемой логики по результатам анализа накопленного в мире опыта применения ПЛИС типа FPGA в составе NIDS.

Прежде, чем перейти непосредственно к принципам создания систем обнаружения вторжений на базе ПЛИС, необходимо рассмотреть несколько существенных моментов. В частности, нужно определить место и роль аппаратно реализованных компонентов в структуре СОВ, которая в общем случае может быть сложной и многоуровневой. Необходимо определиться с

требованиями и основными параметрами, предъявляемыми к такому оборудованию, а также его функциональностью. Далее в работе рассматривается обобщенная структура реконфигурируемой СОВ, некоторые важные ее составные части и сопутствующие вопросы.

1. Предварительный анализ

СОВ различаются по многим критериям, в том числе, по уровню сложности и по структуре.

Система обнаружения вторжений в обязательном порядке включает в себя один или несколько сенсоров и интерфейс с пользователем. В состав сенсора, в свою очередь, в общем случае входят [2]:

- модуль работы с источниками информации;
- подсистема регистрации данных;
- база знаний;
- модуль управления компонентами;
- модуль обнаружения атак;
- модуль реагирования.

В настоящей работе рассматриваются только некоторые из перечисленных выше компонентов, наиболее критичные в плане вычислительных затрат, а именно: модуль обнаружения атак, совмещенный для ускорения работы с базой знаний, в роли которой чаще всего выступает база данных сигнатур известных атак.

В работе [3] был проведен предварительный анализ возможностей программируемой логики и способов ее применения в составе систем обнаружения вторжений. В частности, упоминалось, что главной проблемой при защите от внешних атак, эффективное решение которой могут обеспечить ПЛИС, является существенно ресурсоемкая операция распознавания сигнатур в интенсивном потоке сетевых пакетов.

В зависимости от защищаемого объекта, различают СОВ:

- контролирующие отдельные компьютеры;
- анализирующие пакеты сетевого трафика всей локальной сети.

Наибольший эффект от применения аппаратного решения достигается в сетевых системах обнаружения вторжений. Поэтому в настоящей работе речь пойдет именно о таких системах.

Сетевые СОВ, реально применяемые на практике в настоящее время, подразделяются на два основных класса в зависимости от метода анализа событий:

- использующие сигнатуры (Signature-based IDS);
- выявляющие аномалии (Statistical anomaly based IDS).

Системы выявления аномалий, в отличие от использующих сигнатуры, способны обнаруживать новые, неизвестные ранее атаки, но, на сегодняшний день, вызывают недопустимо много ложных срабатываний. Поэтому под сетевыми СОВ (NIDS) в анализируемых источниках понимались системы, основанные на распознавании сигнатур.

Механизм функционирования сетевой системы обнаружения атак в общем случае состоит из 3-х этапов:

- захват сетевых пакетов (packet capture);
- фильтрация и сборка пакетов (filtering / fragmentation reassembly);
- распознавание (pattern matching).

Самым ресурсоемким является последний этап, который сводится к выполнению большого количества операций сравнения содержимого сетевых пакетов с последовательностями символов из базы данных сигнатур.

Анализ сетевого трафика может осуществляться двумя способами:

- путем тотального захвата и инспектирования всех (необработанных – raw) пакетов сетевого трафика;
- с учетом сетевых протоколов (разборкой заголовков сетевых пакетов).

Системы, основанные на первом способе, распознают большее число атак. Для них не являются препятствием нестандартные номера портов, а также искусственное искажение сетевые пакетов. Но такие СОВ намного более ресурсоемки в своей реализации. По этой причине в исследуемых источниках преимущественно описывались системы, учитывающие протоколы.

2. Предъявляемые требования и основные параметры

Проведенный анализ имеющегося опыта построения сетевых СОВ с применением ПЛИС позволяет сформулировать требования, предъявляемые системами обнаружения вторжений к аппаратным ускорителям, а также основные параметры, по которым следует оценивать их эффективность.

Как указывается в работе [4], производительность СОВ определяется двумя главными характеристиками:

- пропускная способность;
- общее число шаблонов, которые может распознавать система.

Следует заметить, что производительность не является абсолютным показателем, важно также, какой ценой она достигнута, то есть, затраты аппаратуры и энергопотребление. Аппаратные затраты при работе с ПЛИС принято оценивать площадью кристалла, задействованной для реализации конкретного устройства, абсолютной или в процентной доле от общего ресурса микросхемы. В качестве единиц измерения данного показателя используют условные эквивалентные логические элементы (вентили – калька с английской терминологии), системные логические элементы либо некоторые структурные компоненты ПЛИС конкретного семейства конкретного производителя – таблицы соответствия, конфигурируемые логические блоки, секции и т.п. [5]

Важной характеристикой любой сложной системы, к каковым относятся ССОВ, является масштабируемость – способность постепенно наращивать возможности без непропорционально высоких дополнительных затрат. Объем сетевого трафика и количество распознаваемых сигнатур являются постоянно изменяющимися величинами, этот факт невозможно недооценивать.

Специфической чертой реконфигурируемых систем обнаружения вторжений на основе сигнатур является необходимость регулярного добавления в базу данных новых шаблонов, и, как следствие, генерацию и загрузку в ПЛИС новой конфигурации. Удобство и скорость выполнения данной операции существенно влияют на практическую полезность системы.

Из-за недостаточной производительности программных решений большинство современных СОВ являются пассивными, то есть, только сигнализируют о выявленном нарушении безопасности, к тому же, как правило, с существенной задержкой, то есть, не в реальном масштабе времени. Ценность системы обнаружения вторжений намного выше в случае наличия функций предупреждения вторжений (Intrusion Prevention System – IPS)

Как указывалось выше, анализ сетевого трафика на низком уровне (raw) эффективнее, чем на уровне сетевых протоколов в смысле информационной безопасности, но требует намного больших затрат. Поэтому современные ССОВ вынуждены выполнять функции фильтрации и сборки сетевых пакетов (filtering / fragmentation reassembly).

В качестве несущественного, но полезного качества следует упомянуть аппаратную реализацию низкоуровневых сетевых операций ресурсами ПЛИС (так называемый встроенный сетевой интерфейс), что позволяет удешевить техническое решение в целом и повысить его гибкость.

3. Обобщенная структура СОВ на базе ПЛИС

Сформулируем в общем виде состав и структуру аппаратной реализации на ПЛИС системы обнаружения вторжений, отвечающую приведенным выше положениям и требованиям. На рисунке 1 приведена обобщенная структурная схема получившегося решения.

В состав структуры входят:

- модуль приема пакетов;
- классификатор пакетов;
- модуль распознавания;
- модуль генерации тревог;
- схема задержки;
- фильтр пакетов;
- модуль выдачи пакетов.

Последние три компонента присутствуют только в структуре активных ССОВ для реализации функциональности предупреждения вторжений.

Модуль приема пакетов осуществляет низкоуровневый захват сетевых пакетов и их преобразование в более удобный для внутрисхемной обработки тип кодирования, например, из формата XAUI (10 Gigabit Attachment Unit Interface) в формат XGMII (10 Gigabit Media Independent Interface) [6].

Классификатор разбирает пакеты на основе анализа заголовков вплоть до определенного уровня в зависимости от используемого метода обнаружения вторжений [7].

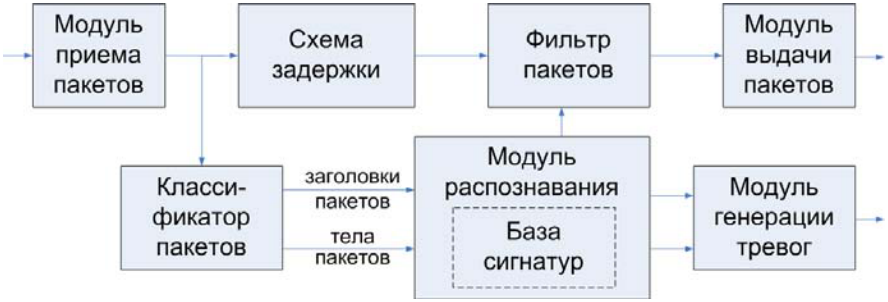

Рис.1. Обобщенная структурная схема ССОВ на базе ПЛИС

Модуль распознавания выполняет самую ресурсоемкую вычислительную операцию поиска сигнатур в соответствии с выбранным алгоритмом. От качества его реализации в значительной степени зависят главные характеристики всей системы обнаружения вторжений: производительность, ресурсоемкость и масштабируемость. Рассмотрение различных возможных алгоритмов распознавания строк в потоке сетевой информации, применяемых в реконфигурируемых СОВ выходит за рамки настоящей работы и будет рассмотрено в последующих публикациях. В общем случае, для работы модуля распознавания необходимы заголовки и содержимое сетевых пакетов, а также информационная база данных правил распознавания сигнатур, включая сами сигнатуры. В зависимости от реализуемого алгоритма данная база либо хранится отдельно, в компонентах внутренней памяти ПЛИС, либо непосредственно "вшита" в распознающую вычислительную структуру [8].

Помимо аппаратуры, реализующей собственно алгоритм поиска вхождения шаблонов в содержимом сетевых пакетов, модуль распознавания в общем случае содержит также схему распознавания заголовков пакетов и детектор правил базы данных сигнатур.

Модуль генерации тревог служит для формирования сообщений об обнаруженных вторжениях. Он идентифицирует вредоносные пакеты и объединяет информацию о типе атаки, поступающую от узла распознавания с дополнительными сведениями из заголовков пакетов, позволяющими идентифицировать источник вторжения. Сформированные сообщения, в зависимости от структуры СОВ, выдаются либо в модуль реагирования данного сенсора, либо через интерфейс пользователя непосредственно администратору безопасности.

Фильтр пакетов служит для пресечения вредоносного трафика путем отбрасывания выявленных пакетов.

Модуль выдачи пакетов реализует преобразование, обратное тому, что выполнялось в модуле приема пакетов.

4. Автоматизированная генерация конфигураций.

Как следует из публикаций, ССОВ на ПЛИС позволяют задействовать многие важные преимущества реконфигурируемой логики, в первую очередь – гибкость и адаптивность. В самом деле, они предоставляют возможность синтезировать аппаратную схему, оптимизированную не просто под конкретную задачу, а под задачу с конкретный набором входных параметров (списком анализируемых сигнатур).

Для того, чтобы эффективно реализовать данное ценное качество, необходимо предпринять дополнительные меры, а именно, автоматизировать процесс генерации конфигураций, загружаемых в ПЛИС [9].

В общем случае, процесс синтеза конфигурации для ССОВ состоит из следующих этапов (рис.2).

Сначала анализируется база данных сигнатур известных на данный момент атак. Помимо собственно шаблонов – последовательностей искомых символов – база содержит также правила их поиска. В результате анализа формируется актуальная таблица правил и другие вспомогательные информационные структуры [6].

В большинстве академических исследованиях по данной теме в качестве наборов сигнатур использовались базы свободно распространяемых систем обнаружения вторжений, таких как Snort, Hogwash, Bro и т.п. [10 – 12].

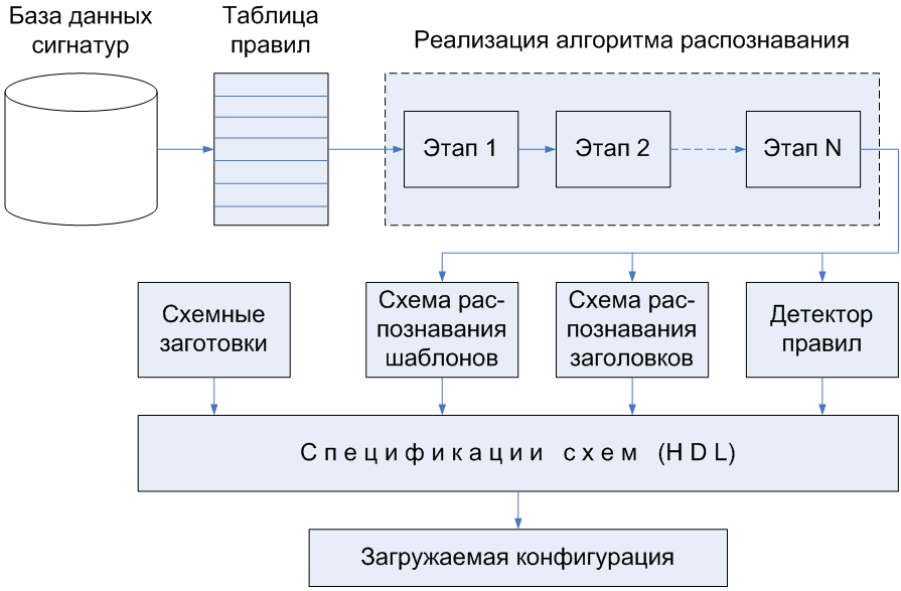

Рис.2. Этапы синтеза конфигураций для ПЛИС в составе ССОВ

Такое решение позволяет, с одной стороны, приблизить проводимые исследования к реальной жизни, благодаря распространенности и интенсивному практическому использованию вышеупомянутых систем. С другой стороны, использование одних и тех же наборов правил в качестве входных параметров облегчает сравнение различных методов, алгоритмов и решений, реализованных в той или иной ССОВ. Более подробное рассмотрение вопросов, связанных с использованием популярных систем обнаружения вторжений с открытым кодом для аппаратной реализации на ПЛИС, также выходит за рамки настоящей работы и планируется к опубликованию в последующих статьях.

Дальнейшие этапы синтеза конфигураций существенно зависят от алгоритмов распознавания, выбранных в качестве основы для данной ССОВ. Они могут состоять из различных шагов и обладать различной сложностью и вычислительной ресурсоемкостью. В общем случае на их выходе формируются следующие структуры:

- схема распознавания шаблонов;
- схема распознавания заголовков;
- детектор правил базы данных сигнатур.

На данной стадии также подключаются фиксированные схемные шаблоны остальных компонентов, не зависящих от набора распознаваемых правил [6].

Далее, по имеющимся структурам составляются спецификации схем, как правило, на одном из языков описания аппаратуры (Hardware Description Language – HDL).

На завершающей стадии из имеющегося HDL-описания синтезируется файл конфигурации, готовый для загрузки в ПЛИС. Данная операция может выполняться либо по обычной схеме – с применением фирменных пакетов САПР конкретного производителя микросхем программируемой логики, либо с привлечением специальных программных средств, разрабатываемых одновременно с ССОВ.

Следует заметить, что процесс автоматизированной генерации конфигураций для систем обнаружения вторжений также требует дополнительного исследования в отдельных публикациях.

Выводы по результатам настоящей работы могут быть сформулированы следующим образом.

В настоящее время мировое научное сообщество уделяет большое внимание проблемам создания на базе ПЛИС высокопроизводительных СОВ сигнатурного типа.

В качестве базы сигнатур для экспериментальных ССОВ на ПЛИС в изученных разработках чаще всего использовалась одна из свободно распространяемых баз данных, поддерживаемых мировым интернет-сообществом на правах программного обеспечения с открытым кодом.

В настоящей работе проанализирован существующий мировой опыт разработки подобных систем. Сформулированы требования и основные технические параметры. Описана обобщенная структура реконфигурируемой сетевой системы обнаружения вторжений. Рассмотрены некоторые важные ее компоненты.

Описана также обобщенная структура процесса автоматизированной генерации конфигураций, загружаемых в ПЛИС сетевой СОВ.

Вместе с тем, в настоящей работе обозначено много моментов, требующих дальнейшего исследования и обобщения, что косвенно свидетельствует о масштабности и актуальности исследуемой проблемы.

1. *Paxson V., Asanovic K., Dharmapurikar S., Lockwood J., etc.* Rethinking Hardware Support for Network Analysis and Intrusion Prevention // USENIX First Workshop on Hot Topics in Security (HotSec), Vancouver, B.C., July 31, 2006.
2. *Лукацкий А.В.* Обнаружение атак. – СПб.: БХВ-Петербург, 2001. – 624 с.
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. *Jung H-J, Baker Z.K., Prasanna V.K.* Performance of FPGA Implementation of Bit-split Architecture for Intrusion Detection Systems // Reconfigurable Architectures Workshop at IPDPS (RAW '06), April 2006.
5. *Максфилд К.* Проектирование на ПЛИС. Курс молодого бойца. – М.: Издательский дом «Додэка-XXI», 2007. – 408 с.
6. *Katashita T., Yamaguchi Y., Maeda A., Toda K.* FPGA-Based Intrusion Detection System for 10 Gigabit Ethernet // IEICE - Transactions on Information and Systems, v.E90-D n.12, p.1923-1931, December 2007.
7. *Jiang W., Prasanna V.* Scalable Multi-Pipeline Architecture for High Performance Multi-Pattern String Matching // IEEE International Parallel and Distributed Processing Symposium (IPDPS '10), April 2010.
8. *Jiang W., Prasanna V.* A FPGA-based Parallel Architecture for Scalable High-Speed Packet Classification // Proceedings of the International Conference on Application-Specific Systems, Architectures and Processors, July 2009, pp.24-31.
9. *Mitra A., Najjar W., Bhuyan L.* Compiling PCRE to FPGA for accelerating SNORT IDS, Proceedings of the 3rd ACM/IEEE Symposium on Architecture for networking and communications systems // December 03-04, 2007, Orlando, Florida, USA.
10. The Open Source Network Intrusion. http://www.snort.org
11. Intrusion Detection System. http://hogwash.sourceforge.net
12. Bro Intrusion Detection System. http://www.bro-ids.org

Поступила 6.10.2010р.