М. Р. Мухтаров

ИСПОЛЬЗОВАНИЕ ПРОТОКОЛА IPFIX ДЛЯ РЕГИСТРАЦИИ РАСПРЕДЕЛЕННЫХ АТАК «ОТКАЗ В ОБСЛУЖИВАНИИ», НАПРАВЛЕННЫХ НА «ОБЛАЧНУЮ ИНФРАСТРУКТУРУ»

Введение

Одной из современных тенденций развития информационных технологий (ИТ) является стремление разработчиков ИТ к объединению различных приложений и служб в так называемые «услуги информационных технологий», или просто ИТ-услуги. Данные консолидации приобретают весьма сложную форму, с одной стороны, а с другой — редуцируются до веб-приложений. Конечным результатом этого процесса в настоящее время стало появление технологии «облачных вычислений» и инфраструктуры «облачных вычислений», которые являются базовым компонентом нового вида ИТ-услуг. Модель, согласно которой данные услуги предоставляются, получила общее название «Приложение как услуга» (англ. Software as a Service — SaaS). SaaS объединяет различные технологии, основной целью которых является решение ряда задач: обеспечение простоты доставки приложений до пользователя, минимизация затрат на обслуживание, упрощение процедуры лицензирования программного обеспечения [1].

Инфраструктура «облачных вычислений» представляет собой совокупность виртуальных машин, распределенных на некотором количестве аппаратного обеспечения (серверов). Количество виртуальных машин, запущенных на одном сервере, зависит от его производительности, нагрузки и других показателей. Количество серверов, задействованных в инфраструктуре «облачных вычислений», зависит от масштаба платформы и решаемых ею задач. Само понятие «компьютерного облака» (англ. Computer Cloud) подразумевает наличие большого количества задействованных физических серверов [2].

Данная технологическая новинка представляет интерес с точки зрения обеспечения информационной безопасности как платформы в целом, так и отдельных ее компонентов. Одной из основных проблем технологии «облачных вычислений» с точки зрения информационной безопасности является архитектура инфраструктурного решения платформы — «облачной инфраструктуры» (англ. Cloud Infrastructure). Она подразумевает коллективный доступ к платформе «облачных вычислений» посредством веб-интерфейса. Иными словами, все пользователи «облачной инфраструктуры» используют общие программные и аппаратные компоненты и общие каналы связи [2].

На данный момент комплексные системы обнаружения и предотвращения сетевых вторжений для «облачной инфраструктуры» только начали свое формирование [2]. Первые исследования в области безопасности «облачных вычислений» датируются 2009 г. Прежде всего, это связано с подготовкой отчета «Риски и рекомендации “облачных вычислений”» рабочей группой ENISA (European Network and Information Security Agency) [3]. Некоторые исследования направлены на изучение различных способов выявления уязвимостей систем такого рода [2, 4]. В ряде работы были предложены методы контроля нарушения правил политики безопасности в рамках «облачной инфраструктуры» [5–7]. Непосредственными объектами исследований являются «облачные инфраструктуры» крупных операторов телематических услуг связи, например Bitbucket и Amazon EC2. «Облачная инфраструктура» этих операторов регулярно подвергается распределенным атакам «отказ в обслуживании», что наносит существенные убытки из-за простоя приложений, виртуализированных в рамках их ресурсов [2, 4]. Например, по данным Arbor Networks Inc., общая мощность атак «отказ в обслуживании» за последние три года увеличилась примерно в три раза. Проблемой в данном случае является надежная регистрация таких атак [4].

Необходимо отметить, что во время распределенной атаки «отказ в обслуживании» происходят изменения количественных характеристик сетевого трафика, что приводит к появлению аномалии в профиле сетевого трафика. Следовательно, методы, основанные на фиксации отклонений от нормального поведения, могут быть эффективны для регистрации распределенных атак «отказ в обслуживании».

В данной работе развивается подход, основанный на фиксации отклонений от нормального поведения профиля сетевого трафика с использованием датчиков протокола IPFIX (структура протокола IPFIX рассмотрена в документе [8]) [9, 11–12]. В работе используется подход размещения датчиков протокола IPFIX на виртуальных сетевых интерфейсах (англ. Virtual Network Interface), предложенный впервые на конференции ICNS 2011 [10]. При этом решена задача надежной регистрации распределенных атак «отказ в обслуживании» внутри «компьютерного облака» с помощью распределенной сети датчиков протокола IPFIX, которые могут быть размещены в составе аппаратных и программных компонентов «облачной инфраструктуры» [10].

Протокол IPFIX был выбран, так как он поддерживается большинством производителей сетевого оборудования, а также в ядре операционной системы Linux [7]. Таким образом, использование протокола IPFIX позволяет разместить датчики в большом количестве возможных точек сбора трафика «облачной инфраструктуры» [10]. Использование данного протокола позволяет построить эталонный профиль сетевого трафика [9–12] и контролировать наличие отклонений при возникновении распределенных атак «отказ в обслуживании».

В данной работе рассматривается структура протокола IPFIX, а также его роль как источника информации заголовков сетевого и транспортного уровня IP-пакетов для целей последующего анализа [8, 9].

1. Регистрация распределенных атак «отказ в обслуживании» в рамках «облачной инфраструктуры»

Рассмотрим распределенную атаку «отказ в обслуживании» (далее – DDoS-атака) по технологии ее реализации. DDoS-атака представляет собой лавинообразный поток запросов, поступающих на атакуемый объект с множественных источников. Содержание и форма этих запросов полностью легитимны. Однако объект атаки при этом недоступен, что говорит о вредоносности таких запросов. При этом применение метода сигнатурного поиска будет неэффективным, так как он основывается на сравнении формы и содержания запросов, поступающих к защищаемой системе. Следовательно, можно сделать вывод о том, что системы предотвращения вторжений, основанные на сигнатурном поиске, будут обладать низким показателем способности произвести обнаружение распределенной атаки «отказ в обслуживании».

Именно данный факт привел исследователей и разработчиков систем сетевой безопасности к выводу о возможности использования методов, основанных на отклонении от нормального функционирования [13, 14]. Описанная группа методов хорошо работает применительно к сетевому трафику, а именно к количественным оценкам объема сетевого трафика во времени. Кроме того, методы, основанные на регистрации аномалий, обладают способностью на ранней стадии эффективно оповещать о распределенных атаках «отказ в обслуживании» [7, 8, 14].

Для обеспечения раннего оповещения распределенных атак «отказ в обслуживании» необходимо использовать распределенный подход. Получение информации из всех возможных точек сбора данных о сетевом трафике позволяет существенно улучшить результативность обнаружения атак [14].

Традиционные системы обнаружения вторжений осуществляют прямой перехват трафика [14]. Для этого потребуется размещение большого количества устройств перехвата по всей сети [14].

Традиционные системы обнаружения вторжений часто требуют установки агента на контролируемую систему или размещения отдельного стоящего блока. В рамках виртуализированной

среды «облачной инфраструктуры» данный подход трудно реализовать. Для обоснования этого факта рассмотрим схему организации типичной инфраструктуры «облачных вычислений» (рис. 1).

На представленной схеме можно выделить основные компоненты: физический сервер, физическая сеть передачи данных, виртуальные локальные вычислительные сети (ВЛВС), ВЛВС системы хранения данных (СХД), виртуальные машины (ВМ) потребителей, хранилища данных потребителей (/dev/sd*).

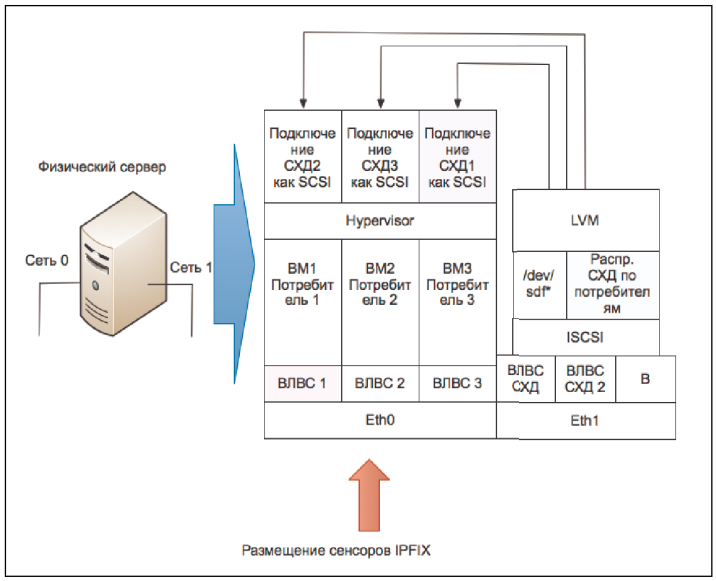

Рис. 1. Схема размещения виртуальных машин на физическом сервере

Анализ этой схемы показывает, что сеть передачи данных в рамках инфраструктуры «облачных вычислений» использует помимо физической сети также виртуальную. Количество виртуальных интерфейсов существенно превышает количество физических. Для контроля каждого потребителя оператора телематических услуг связи потребовалось бы очень большое количество датчиков традиционной системы обнаружений вторжений.

Выходом из положения является использование датчика на основе протоколов сетевой статистики. В данной работе предлагается использовать протокол IPFIX [8], так как он базируется на полностью открытом стандарте IETF и описан в документе RFC5101, находящемся в свободном доступе. Датчик IPFIX может быть размещен стандартным образом на интерфейсе Linux, не оказывая влияния на производительность платформы. Оценка производительности при использовании IPFIX приведена в работе [10].

2. Построение эталонного профиля и регистрация распределенных атак «отказ в обслуживании» с помощью протокола IPFIX

Протокол IPFIX позволяет передавать данные измерения сетевого трафика от сетевого оборудования или программного датчика к коллектору-IPFIX. Коллектор-IPFIX – это компонент, который представляет собой серверное приложение, ожидающее входящие данные от сетевого оборудования. Ниже приведен пример структуры пакета IPFIX/Netflow версии 9 (рис. 2).

Согласно спецификации протокола IPFIX, измерения сетевого трафика группируются в специальный объект, называемый «Flow», или «поток» IPFIX. Трафик группируется в «поток» IPFIX по принадлежности к текущей сессии. Результаты измерений по каждой сессии TCP или группе UDP-дейтаграмм датчик IPFIX группирует в «поток» IPFIX. К «потоку» прикладывается количество пакетов и байт, переданных в данный период. Собранный поток пересылается датчиком в коллектор IPFIX [8].

Информацию, предоставляемую протоколом IPFIX, можно анализировать с помощью одного из статистических методов. В рамках данной работы был разработан алгоритм, который позволяет производить регистрацию сетевых аномалий, развивающихся с низкой интенсивностью. Предложенный алгоритм основан на принципе максимума энтропии [11].

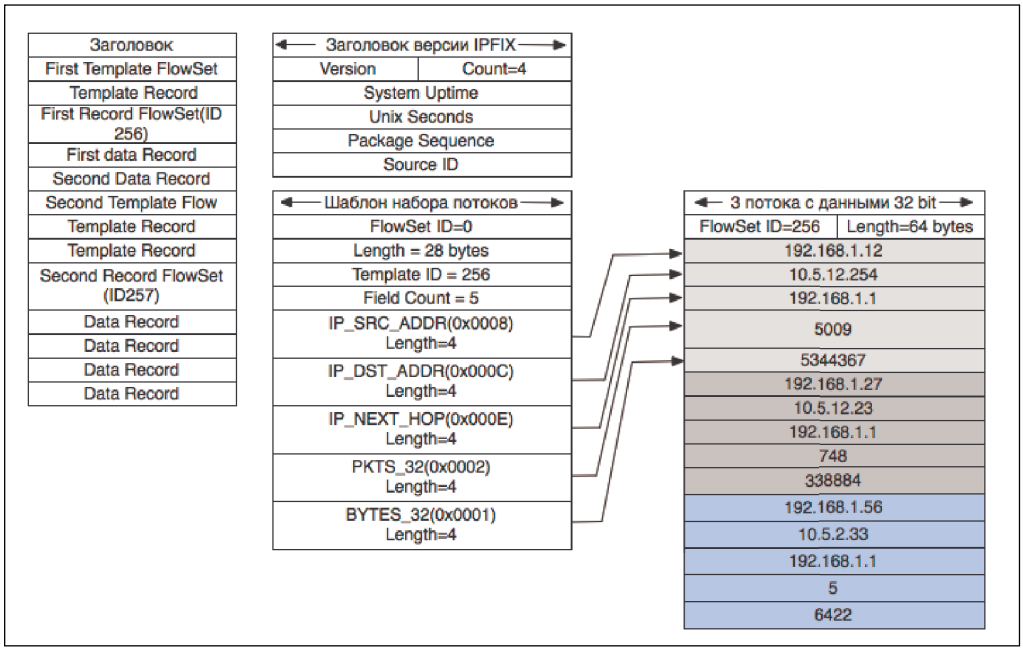

Рис. 2. Структура пакета IPFIX/Netflow версии 9

Алгоритм предполагает использование нескольких этапов: классификация данных, предоставляемых протоколом IPFIX; построение эталонного профиля количественных характеристик сетевого трафика для каждого класса; сравнение текущих показаний объемов сетевого трафика с эталонным профилем. В данной работе разберем первую часть алгоритма, относящуюся к классификации информации о сетевом трафике.

Данные об объемах сетевого трафика разбиваются на классы по типу протокола и портам. Период времени сбора начальных данных для работы алгоритма задается пользователем и должен быть уточнен для конкретного объекта наблюдений [11]. Классы сетевого трафика также задаются пользователем и могут различаться для различных систем. Прежде всего, они зависят от типа используемых сетевых соединений и сетевых портов в рамках работы системы. Если говорить об «облачной инфраструктуре», то это порты протокола TCP и UDP, отвечающие за передачу сетевого трафика по протоколам, используемым для доступа к виртуальной среде и передачи данных внутри нее.

В блок-схеме алгоритма классификации трафика (рис. 3) каждая запись IPFIX сравнивается с указанным классом. Работа алгоритма подразумевает организацию двух циклов — считывания очередного потока IPFIX и цикла сравнения входящих данных с заданными классами. В алгоритме проверяются три условия: принадлежность данных о сетевом трафике из потока к классу, условие перехода к следующему потоку IPFIX и условие окончания входных данных.

В результате работы алгоритма строится выборочное распределение вхождения трафика в каждый класс. Полученный эталонный профиль используется для сравнения текущих показаний сетевого трафика. Для решения задачи сравнения двух распределений трафика требуется решить задачу поиска различий между двумя распределениями. Выбор математического метода для определения различий эталонного и наблюдаемого распределений трафика является темой дальнейших исследований.

Заключение

Использование современных телематических услуг связи на основе «облачных вычислений» требует дополнительных исследований проблем обеспечения информационной безопасности таких технологий. В настоящее время выявлено достаточно большое количество рисков, связанных с эксплуатацией данных систем.

Использование традиционных систем обнаружения вторжений не обеспечивает достаточной надежности выявления распределенных атак «отказ в обслуживании».

Рассмотренный в данной работе подход, позволяющий организовать распределенный сбор информации о сетевом трафике, основан на использования протокола IPFIX. Формат данных IPFIX/Netflow удобен для статистического анализа.

Применение протокола IPFIX позволяет организовать распределенный сбор информации о сетевом трафике, провести классификацию этой информации, построить эталонный профиль количественных характеристик сетевого трафика для каждого класса и осуществить сравнение текущих показаний объемов сетевого трафика с эталонным профилем. Реализация данного алгоритма даст возможность повысить надежность регистрации распределенных атак «отказ в обслуживании» на «облачную инфраструктуру». В работе была рассмотрена блок-схема первой части предлагаемого алгоритма.

Датчики IPFIX могут быть внедрены в уже существующие сети передачи данных и виртуальные инфраструктуры.

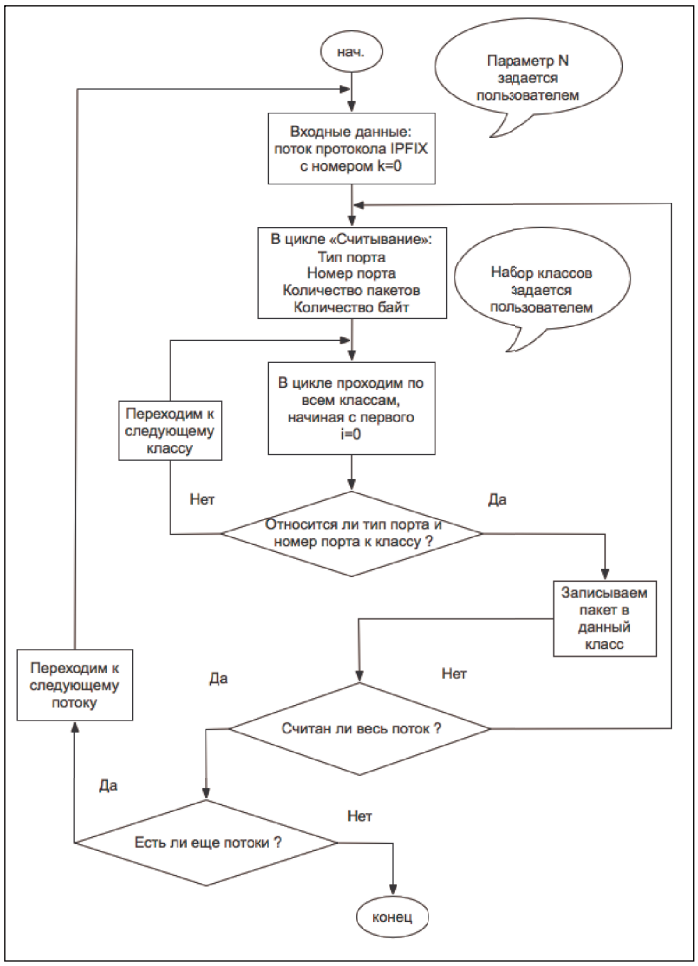

Рис. 3. Блок-схема алгоритма классификации трафика

СПИСОК ЛИТЕРАТУРЫ:

1. “Software as a Service (SaaS) - Cloud Taxonomy”. URL: http:// http://cloudtaxonomy.opencrowd.com/taxonomy (2010) (Дата обращения: 24 апреля 2011 г.).
2. *Tay L., Kotadia M.* Data breaches to cost more in the cloud. URL: http://www.securecomputing.net.au (2010) (Дата обращения: 23 марта 2011 г.).
3. *Catteddu D., Hogben G.* Cloud Computing “Benefits, risks and recommendations for information security”. URL: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport (2009) (Дата обращения: 23 марта 2011 г.).
4. *McNamara P.* DDoS attack against Bitbucket darkens Amazon cloud. URL: http://www.networkworld.com (2009). (Дата обращения: 23 марта 2011 г.).
5. *Molnar D., Schechter S.* Self Hosting vs. Cloud Hosting: Accounting for the security impact of hosting in the cloud. // Proceedings of the Ninth Workshop on the Economics of Information Security. Microsoft Research. 2010. URL: http://research.microsoft.com/apps/pubs/default.aspx?id=132318 (2010) (Дата обращения: 25 марта 2011 г.).
6. *Vadhat A.* The achilles’ heel of performance isolation in the cloud. URL: http://idleprocess.wordpress.com/2010/01/17/the-achilles-heel-of-performance-isolation-in-the-cloud (2010) (Дата обращения: 10 сентября 2011 г.).
7. *Berger S., Caceres R., Goldman K. and others.* Security for the cloud infrastructure: Trusted virtual data center implementation // IBM J. RES & DEV. 2009. Vol. 53. № 5.
8. *Claise B. Ed.* RFC 5101: Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information URL: http://tools.ietf.org/html/rfc5101 (2008) (Дата обращения: 25 сентября 2011г.).
9. *Leinen S.* RFC3955: Evaluation of Candidate Protocols for IP Flow Information. URL: http://www.ietf.org/rfc/rfc3955.txt (2004) (Дата обращения: 25 сентября 2011 г.).
10. *Mukhtarov M., Miloslavskaya N., Tolstoy A.* Network security threats and Cloud Infrastructure Services Monitoring // ICNS 2011, The Seventh International Conference on Networking and Services. 2011. P. 141–145.
11. *Gu Y., McCallum A., Towsley D.* Detecting anomalies in network traffic using maximum entropy // Tech. rep. Department of Computer Science. UMASS, Amherst, 2005.
12. Cisco-Arbor Clean Pipe Solution 2.0 White Paper. URL: http://www.arbornetworks.com/index.php?option=com_docman&task=doc_download&gid=448 (Дата обращения: 25 сентября 2011 г.).
13. *Chen Y.* Distributed Change-Point Detection of DDoS Attacks: Experimental Results on DETER Testbed // DETER Community Workshop on Cyber Security Experimentation and Test, in conjunction with USENIX Security Symposium, Boston, 2008.
14. *Lee W., Xiang D.* Information-theoretic measures for anomaly detection // Proceedings of the IEEE Symposium on Security and Privacy. IEEE Computer Society. 2001. P. 130.