Отзыв официального оппонента

Волконского Владимира Юрьевича на диссертационную работу
Маркина Юрия Витальевича
«Методы и средства углубленного анализа сетевого трафика»,
представленную к защите на соискание ученой степени кандидата технических наук по специальности 05.13.11 – «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей»

Современное человечество с каждым днем все более активно использует компьютерные сети. При этом сетевой трафик постоянно увеличивается в объеме, усложняется структура сетевых сообщений, возрастают угрозы безопасности. Углубленный анализ сетевого трафика становится крайне актуальной задачей по многим причинам. Во-первых, с помощью сетевых сообщений могут осуществляться мошеннические действия и зловредные проникновения, которые необходимо предотвращать. Во-вторых, способ передачи больших сообщений параллельными порциями требует их правильного упорядочивания при приеме. В-третьих, широко используются туннельные протоколы, требующие обеспечения безопасности таких соединений. В-четвертых, все более широкое использование шифрованных сообщений требует анализа сертификатов безопасности и проверки надежности криптоалгоритмов. Наконец, углубленный анализ трафика необходимо выполнять не только «на лету» (on-line), но и при его сохранении (off-line) для выявления сложных и опасных проблем взаимодействия в сети. Метод решения всех перечисленных задач рассматривается в представленной диссертационной работе Маркина Ю.В., что, безусловно, *подтверждает ее актуальность*.

Безусловной *научной новизной* обладает предложенная в работе *модель* представления данных, позволяющая единообразно описывать разбор заголовков произвольного стека сетевых протоколов, а также *алгоритмы восстановления* переупорядоченных пакетов и вся архитектура системы углубленного анализа, единая для режимов работы on-line и off-line.

Диссертационная работа состоит из введения, пяти глав, заключения и списка литературы из 53 наименований.

Во введении обосновывается актуальность работы, определяются цели и задачи работы, формулируются основные научные результаты, обосновываются теоретическая и практическая ценность, а также данные об апробации работы.

Первая глава посвящена обзору и анализу возможностей существующих систем углубленного анализа сетевого трафика и систем обнаружения вторжений. В ней рассмотрены *особенности передачи* сетевого трафика, *сформулированы функциональные требования* к его анализаторам и *определен способ оценки* современных методов разбора, базирующийся на наборе сетевых трасс и изучении исходного кода и документации известных анализаторов.

Результаты анализа трех (в автореферате четырех) систем (Snort, Bro, Wireshark, и еще только в автореферате ntopng) подтверждают неполное соответствие каждой из них сформулированным требованиям, что является основанием для разработки новой модели представления данных и системы анализа трафика на ее основе.

Во второй главе рассматривается предложенная в работе *новая модель* представления разбора сетевого трафика, удовлетворяющая требованиям, сформулированным в главе 1. Для этого разобранный сетевой пакет представляется *в виде дерева блоков*, определяемых классом *Block*, диаграмма классов которого подробно рассмотрена и обоснована. Для описания *логических соединений* используется специальная диаграмма классов, в которой важную роль играют *контекстная группа* и *ключевая группа*. Введение понятия *распознаватель*, обеспечивает разбор пакетов произвольного стека протоколов. В этой главе также приведен *алгоритм восстановления потоков*, при использовании которого не возникает неопределенности, к какой единице передачи (PDU – Protocol Data Unit) необходимо отнести пакет, полученный в неправильном порядке. Эта модель и механизм распознавания позволяют естественным образом анализировать трафик вложенных туннелей любой конфигурации, восстанавливать поток данных всех соединений с переупорядоченными пакетами, а также обнаруживать повторные и потерянные пакеты.

В третьей главе представлена архитектура модульной системы анализа, позволяющая обходиться *единым комплектом исходных кодов разборщиков* протоколов как в on-line, так и в off-line режимах. Необходимость наращивания системы новыми разборщиками не требует внесения изменений в уже существующие, что обеспечивается механизмом их связывания на базе применения распознавателей. Программный интерфейс системы позволяет регистрировать разборщики и распознаватели, создавать все компоненты структурной модели, управлять восстановлением потоков. Для увеличения базы поддерживаемых протоколов системы разработан *инструмент портирования разборщиков* анализатора Wireshark, который позволил автоматически перенести модуль разбора протокола CAST, *автоматически* преобразовав исходный код объемом 1457 строк в код объемом 894 строки, реализация которого потребовала бы значительных усилий специалиста высокой квалификации.

В четвертой главе описываются разработанные on-line и off-line анализаторы трафика. Структура и компоненты *on-line анализатора* должны обеспечивать выполнение анализа в режиме реального времени со скоростью поступления сетевого трафика. Важнейшей задачей при этом является *правильное управление ресурсами*, в первую очередь оперативной памятью, перераспределяя ее наиболее рационально между объектами с относительно короткими и более долгими временами жизни. При возникновении несоответствия фактических данных описанию протокола в модуле разбора такие пакеты помещаются в файл для последующего off-line анализа. *Off-line*

анализатор предназначен для разработки и отладки модулей разбора. Для него важен хороший *графический интерфейс*, который позволяет анализировать дерево блоков, отлаживать разборщики с использованием журнала ошибок разбора, анализировать граф сетевых узлов, *анализировать шифрованные данные*. *Интерактивный разбор*, требуемый в случаях, когда заложенные в систему эвристики не учитывают всех возможных вариантов содержимого сетевого пакета, предназначен для аналитика, который может *передать системе файл с дополнительными подсказками*.

В пятой главе представлены *результаты практического применения* разработанной системы. Демонстрируется восстановление переупорядоченных пакетов, анализ зашифрованного SSL трафика, возможность извлечения файлов при проведении on-line анализа. Наибольший интерес представляет *результат обратной инженерии закрытого протокола ботнета* rbot, который позволил восстановить основные команды управляющего протокола ботнета.

В заключении приводятся основные результаты работы, которые выносятся на защиту:

1. Разработанная модель представления сетевых пакетов, учитывающая потери/переупорядочивание отдельных пакетов, сжатие и шифрование данных, вложенное тунеллирование.
2. Разработанный алгоритм восстановления потоков данных для протоколов произвольного уровня, в том числе прикладного, устойчивый к потерям отдельных сетевых пакетов, а также к их переупорядочиванию.
3. Разработанная архитектура системы углубленного анализа сетевого трафика, позволяющая разрабатывать и отлаживать модули поддержки протоколов на предварительно сохраненном трафике и впоследствии использовать эти модули в режиме on-line/
4. Разработанные и реализованные программные инструменты для проведения углубленного анализа сетевого трафика в on-line и off-line режимах.

Несмотря на высокое качество диссертационной работы в ней следует отметить ряд недостатков:

1. В диссертации не указан личный вклад автора, это сделано только в автореферате.
2. В диссертации в списке литературы отсутствуют ссылки на работы автора (они указаны только в автореферате), поэтому по тексту диссертации трудно определить, какие ее положения были опубликованы.
3. В анализе известных инструментов, приведенном в первой главе диссертации, меньше инструментов, чем в автореферате, хотя вывод по результатам их анализа совпадает.
4. В первой главе использованы 3 набора сетевых трасс, по результатам анализа которых устанавливаются недостатки рассмотренных известных инструментов, однако аналогичные данные не приведены для предложенной

в работе системы.

5. В работе используется много англоязычных сокращений, но при этом отсутствует их список, что иногда затрудняет восприятие материала.

Отмеченные недостатки не влияют на общую положительную оценку работы.

Диссертационная работа Маркина Ю.В. является законченным научным исследованием, а реализованные и практически испытанные инструменты подтверждают ее *практическую ценность*. *Достоверность работы* полностью подтверждается проведенными экспериментами. Полученные автором результаты отражены в опубликованных им работах и *прошли апробацию* на нескольких конференциях.

Автореферат с учетом отмеченных в нем дополнений *полно и правильно* отражает содержание диссертационной работы.

Диссертационная работа Маркина Юрия Витальевича соответствует всем требованиям ВАК РФ, предъявляемым к диссертациям на соискание ученой степени кандидата технических наук, а ее автор, Маркин Юрий Витальевич, заслуживает присуждения ему ученой степени кандидата технических наук по специальности 05.13.11 – «математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей».

Кандидат технических наук, старший научный сотрудник, начальник отделения «Системы программирования» публичного акционерного общества «ИНЭУМ им. И.С. Брука» В.Ю. Волконский

Подпись кандидата техничес
Волконского В.Ю. заверяю, зам. ге
директора ПАО «ИНЭУМ им. И.С. В.И. Перекатов

«5» мая 2017 г.