ОТЗЫВ
официального оппонента 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»

Актуальность темы исследования. Представленная диссертационная работа посвящена исследованию и разработке методов анализа сетевого трафика, обеспечивающих повышение качества разбора сетевых пакетов, а также позволяющих автоматизировать расширение функциональности сетевых анализаторов. Анализ трафика лежит в основе решения таких востребованных прикладных задач, как обеспечение информационной безопасности в рамках внутренней сети предприятия, обнаружение неполадок в работе сетевого оборудования, повышение качества услуг, предоставляемых интернет провайдерами и др. Тем самым, задача анализа сетевого трафика может быть отнесена к комплексной проблеме обеспечения кибербезопасности, успешное решение которой представляет один из глобальных вызовов для успешного развития современного общества.

Качественное решение задач информационной безопасности предполагает возможность анализа сетевого трафика, который может генерироваться с использованием разных протоколов различных уровней. Если проблемы в работе сети могут быть устранены с помощью данных канального и сетевого уровней OSI, то для обнаружения и защиты от вторжений, как правило, требуются данные вышележащих протоколов – сеансового или прикладного уровней. Решение проблемы анализа сетевого трафика при подобном разнообразии протоколов обеспечивается за счет декомпозиции: прикладные задачи анализа используют уже готовые результаты разбора сетевого трафика; непосредственный же анализ сетевого

трафика обеспечивается отдельными комплексами сетевых анализаторов. Такой подход позволяет проводить разбор трафика в рамках некоторого единого сетевого анализатора и обеспечивать все остальные инструменты необходимыми им данными, извлеченными из сетевого трафика. В таком случае упрощается дальнейшее расширение функциональности системы: поддерживать работу с новыми протоколами нужно будет только в инструменте, проводящем разбор сетевого трафика.

Сетевые анализаторы, необходимые для подобной декомпозиции проблемы анализа сетевого трафика, уже имеют ряд реализаций. Коммерческие разработки выполнены на высоком профессиональном уровне, однако являются закрытыми для развития сторонними разработчиками. Свободно-распространяемые разработки обладают, как правило, существенно меньшими возможностями. Тем самым, тема диссертационной работы Маркина Ю.В. по разработке эффективных методов и программных средств углубленного анализа сетевого трафика является **актуальной и значимой**.

К **основным результатам**, полученным Маркиным Ю.В. в ходе выполнения диссертационного исследования, следует отнести:

1. Модель представления данных, получаемых в результате разбора сетевого трафика. В разработанной модели учитываются многие сложные варианты сетевого трафика, в которых возможна потеря/переупорядочивание отдельных пакетов, может использоваться сжатие и шифрование данных, может применяться вложенное туннелирование и т.п.

2. Алгоритм восстановления потоков данных для протоколов произвольного уровня. Разработанный алгоритм является устойчивым к потерям и переупорядочиваниям отдельных сетевых пакетов.

3. Архитектура системы углубленного анализа сетевого трафика, позволяющая разрабатывать и отлаживать модули поддержки протоколов на

предварительно сохраненном трафике (offline) и впоследствии использовать эти модули в режиме online.

4. Программные инструменты для проведения углубленного анализа сетевого трафика в online и offline режимах.

Научная новизна результатов, представленных в диссертационной работе Маркина Ю.В., заключается в разработке модели представления данных, в разработке устойчивого алгоритма восстановления потоков данных, в разработке архитектуры программной системы анализа сетевого трафика, предусматривающей возможность использования одних и тех же разборщиков сетевых протоколов при проведении анализа в online и offline режимах.

Модель и алгоритм реализованы в виде динамической библиотеки и интерфейса для ее использования в составе программной системы анализа сетевого трафика. Выполненные вычислительные эксперименты подтверждают адекватность разработанного подхода и эффективность реализованных программных средств для углубленного анализа сетевого трафика.

Структура и содержание работы. Диссертация состоит из введения, пяти глав, заключения и списка литературы.

Первая глава посвящена обзору существующих инструментов, выполняющих разбор сетевых пакетов. Характерная особенность, присущая всем рассмотренным анализаторам, состоит в том, что они не предполагают предоставление доступа к результатам разбора. Из этого можно заключить, что:

- при необходимости добавления поддержки нового протокола потребуется разработать разборщик для каждого из инструментов;
- сторонние анализаторы не смогут воспользоваться результатами разбора, проводимого рассмотренными инструментами.

В результате выполненного анализа отмечается, что разбор пакетов в рассмотренных инструментах проводится недостаточно точно, поскольку не полностью учитываются такие побочные эффекты, сопровождающие передачу данных по сети, как фрагментация данных, переупорядочивание отдельных пакетов.

Во **второй главе** описывается разработанная автором модель представления сетевых данных, позволяющая унифицировано описывать разбор произвольного стека протоколов, а также его результаты. Проблема обработки переупорядоченных пакетов решается путем введения потоков, предназначенных для склейки данных, передаваемых в разных пакетах по частям. Разработанный алгоритм восстановления потоков обеспечивает возможность корректного извлечения данных протокола следующего уровня стека.

Третья глава посвящена архитектуре разработанной системы анализа. В состав системы входят модули разбора и распознавания, а также ядро, обеспечивающее их согласованную работу. Модель представления данных и алгоритм восстановления потоков реализованы в рамках ядра. Разборщики заголовков сетевых протоколов реализуются в виде модулей, подключаемых динамически. Важным аспектом архитектуры является разработанный механизм связывания разборщиков заголовков сетевых протоколов.

В **четвертой главе** рассматриваются разработанные программные инструменты для проведения анализа сетевого трафика в online и offline режимах. Важная особенность этих инструментов состоит в том, что для разбора в них используются одни и те же исходные коды разборщиков, чего удалось достичь благодаря различной для online и offline режимов реализации функций API разбора в ядре.

Пятая глава посвящена примерам практического применения разработанных инструментов. Приведен пример корректного восстановления потоков данных, которые не были восстановлены анализатором Wireshark. Показана возможность работы с зашифрованным SSL-трафиком путем

загрузки в систему недостающего для проведения разбора ключа шифрования. Пример с сохранением PNG-файлов демонстрирует возможности по извлечению высокоуровневых данных из трафика. Описана последовательность действий и разработка разборщика закрытого протокола, используемого ботнетом Rbot.

Замечания к диссертационной работе. Диссертационная работа Маркина Ю.В. выполнена на высоком научно-техническом уровне, содержание диссертации имеет четкую структуру, хорошо и понятно изложено. Наряду с отмеченными положительными моментами по диссертационной работе могут быть сделаны следующие замечания:

1. В тексте диссертации отсутствует информация о статьях, опубликованных автором, сведения о публикациях присутствует только в автореферате.

2. В главе 2 не приводится описание результатов разбора сетевых пакетов.

3. В главе 5 при демонстрации работоспособности разработанных программных средств отсутствуют сведения об их вычислительной трудоемкости.

4. В диссертации не рассмотрены возможные способы подключения разработанного сетевого анализатора в сеть и не указаны необходимые для этого технические средства.

Перечисленные замечания не снижают качества выполненного научно-технического исследования на актуальную тему и не влияют на общую положительную оценку работы.

Заключение по диссертационной работе. Диссертация Маркина Юрия Витальевича «Методы и средства углубленного анализа сетевого трафика» является самостоятельной законченной научно-квалификационной работой. Представленные в работе результаты имеют существенное значение для построения анализаторов сетевого трафика с возможностью

автоматизированного расширения их функциональности. Основные результаты диссертации опубликованы в 7 научных работах, из них 4 в журналах из перечня изданий, рекомендованных ВАК.

Диссертационная работа соответствует всем требованиям ВАК РФ, предъявляемым к диссертациям на соискание ученой степени кандидата технических наук, а 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».

Директор Института информационных технологий,
математики и механики Национального исследовательского
Нижегородского государственного университета имени Н. И. Лобачевского,
зав. кафедрой Программной инженерии, д.т.н., проф.
г. Нижний Новгород, пр. Гагарина, 23
Тел.: (831) 462-30-85, gergel@unn.ru

Гергель В.П.