МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования
«Ижевский государственный технический университет имени М.Т.Калашникова»
(ФГБОУ ВПО «ИжГТУ имени М.Т.Калашникова»)

Студенческая ул., д. 7, г. Ижевск, УР, 426069
Тел. (3412) 58-53-58, 58-88-52, 58-28-60
Факс: (3412) 50-40-55
e-mail: info@istu.ru http://www.istu.ru
ОКПО 02069668 ОГРН 1021801145794
ИНН/КПП 1831032740/183101001

_____ № _____

На № _____ от _____

ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова»

Ученому секретарю совета Д.501.002.16
А.А.Корневу

119991, Москва, ГСП–1, Ленинские горы д. 1,
ФГБОУ ВО МГУ имени
М. В. Ломоносова, Механико-математический факультет

ОТЗЫВ

на автореферат диссертации Александрова Д.Е. «Сложность распознавания принадлежности слова регулярному языку в системах обнаружения вторжений», представленной на соискание ученой степени кандидата физико-математических наук по специальностям 05.13.17 — теоретические основы информатики и 05.13.19 — методы и системы защиты информации, информационная безопасность

Анализ и фильтрация сетевого трафика является одной из важнейших задач обеспечения информационной безопасности в компьютерных сетях. Для исследования сетевого трафика на предмет вредоносных действий обычно используются сетевые системы обнаружения и предотвращения вторжений с базами сигнатур, задаваемыми регулярными выражениями. Регулярные языки, соответствующие объединениям выражений баз сигнатур, представляют собой множества, чаще всего бесконечные, всех строковых данных, которые определяются системой как вредоносные. Для проверки принадлежности данных сетевого трафика регулярным языкам строятся соответствующие распознающие детерминированные конечные автоматы. Несмотря на очевидное преимущество такого подхода, при котором сложность линейна по времени относительно длины проверяемой строки, возникает проблема пространственной сложности — проблема большого числа состояний распознающего конечного автомата, размещаемого в памяти вычислительной системы.

В диссертационной работе Д.Е. Александрова рассматривается класс регулярных выражений вида $.*R_1.*R_2.*$, распространённых среди систем активного аудита. Известно, что регулярные выражения такого вида подвержены проблеме «экспоненциального взрыва» — проблеме экспоненциального роста числа состояний распознающего конечного автомата относительно числа регулярных выражений. Автором предложен метод модификации пар выражений данного вида, который позволяет снизить влияние проблемы «экспоненциального взрыва» на распознающий автомат. Д.Е. Александровым были выведены оценки эффективности разработанного метода по снижению числа состояний автомата и оценки вероятности ошибочного срабатывания при предложенной аппроксимации языков. Кроме того, автором были получены практические результаты применения предложенного метода на регулярных выражениях сетевой системы обнаружения вторжений Snort, подтверждающие эффективность метода.

Список научных статей, опубликованных соискателем, позволяет сделать вывод о том, что все выносимые на защиту результаты принадлежат автору, опубликованы в ведущих рецензируемых изданиях и являются новыми. Их достоверность и строгая математическая обоснованность не вызывает сомнений.

Считаю, что работа Д.Е. Александрова является законченным научным исследованием, результаты которого имеют важное теоретическое и практическое значение.

К сожалению, автором были рассмотрены результаты применения метода к базе сигнатур только одной из систем обнаружения вторжений. Однако данный недостаток не влияет на общую положительную оценку работы.

Работа удовлетворяет требованиям, предъявляемым к кандидатским диссертациям, а её автор, Д.Е. Александров, заслуживает присуждения искомой степени кандидата физико-математических наук.

Профессор кафедры «Программное обеспечение» ИжГТУ,
к.т.н., профессор Владимир Георгиевич Тарасов

Подпись Тарасова В.Г. удостоверяю.
Ученый секретарь ИжГТУ д.т.н., профессор В.А. Алексеев