TECHNISCHE UNIVERSITÄT DRESDEN

Faculty of Science Institute of Algebra

Technische Universität Dresden, 01062 Dresden

Dr. Dr.
Artem Revenko
Telefon:
E-Mail: artem_viktorovich.revenko@mailbox.tu-dresden.de

ОТЗЫВ на автореферат диссертационной работы Александрова Дмитрия Евгеньевича «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.

Dresden, 25.08.2015 Ревенко

В силу широкого распространения сетевых технологий в современном мире одной из главных задач в области информационной безопасности стала задача фильтрации сетевого трафика. Фильтрация трафика с целью обнаружения и предотвращения вторжений осуществляется в большинстве систем активного аудита путем сравнения входных данных (например, сетевых пакетов) с регулярными выражениями, составляющими базы сигнатур систем. Для сравнения данных с выражениями используются конечные автоматы. При таком сравнении зачастую возникает проблема экспоненциального взрыва — экспоненциального роста числа состояний распознающего автомата, что в свою очередь влечет высокий рост объема памяти, который необходим для функционирования автомата.

В диссертационной работе Александрова Д.Е. представлен метод, позволяющий снизить влияние проблемы экспоненциального взрыва на наборы регулярных выражений вида $.*R'.*R''.*$. Метод, предложенный автором, состоит в модификации пар регулярных выражений таким образом, что множество распознаваемых слов относительно несильно расширяется, а число состояний автомата существенно снижается. В работе показывается, что наборы регулярных выражений рассматриваемого вида, встречающиеся на практике в системах обнаружения и предотвращения вторжений, подвержены проблеме экспоненциального роста числа состояний распознающего автомата, что свидетельствует о том, что решение проблемы для выражений данного вида представляет теоретический и практический интерес. Александровым Д.Е. выведены оценки, обосновывающие эффективность разработанного метода, а также предложен вычислительно простой способ достаточно точного предсказывания относительного роста регулярных языков при модификации пары выражений. Также на основании полученных результатов автором был разработан программный комплекс для работы с наборами регулярных выражений рассматриваемого вида, результаты применения которого к реальным выражениям сетевой системы обнаружения вторжений представлены в работе.

К недостатку работы можно отнести неявное предположение автора о равномерном распределении входных данных, которое используется в главе 5 при оценке негативного эффекта расширения регулярного языка. При этом данный недостаток не снижает общий высокий уровень работы и обозначает возможное направление дальнейших исследований.

На основании автореферата можно сделать вывод, что диссертационная работа Александрова Д.Е. является законченным научным исследованием и удовлетворяет формальным требованиям, которые предъявляет ВАК к диссертациям на соискание ученой степени кандидата физико-математических наук.