О Т З Ы В

официального оппонента на диссертацию

Гайворонской Светланы Александровны

«Исследование методов обнаружения шеллкодов в высокоскоростных каналах передачи данных»,

представленную к защите на соискание ученой степени

кандидата физико-математических наук по специальности 05.13.11 – математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей.

В диссертационной работе Гайворонской С.А. рассматривается проблема обнаружения вредоносного исполнимого кода, эксплуатирующего ошибки работы с памятью. Подобный код принято называть шеллкодом. Атакам, использующим уязвимости работы с памятью, уже более 10 лет, первая публикация относится к 1996 году. С тех пор появилось не мало работ, посвященных изучению способов эксплуатации ошибок работы с памятью; проблемам автоматического обнаружения подобных уязвимостей в исходных кодах программного обеспечения; механизмов защиты уровня операционных систем, в результате которых эксплуатация ошибок работы с памятью либо значительно усложняется, либо становится невозможной. Эти работы носят, в некотором смысле, рассматривают частные случаи этой проблемы. В диссертации проблема эксплуатации ошибок работы с памятью рассматривается в наиболее общем случае: обнаружение и фильтрация шеллкодов при их транспортировке. Традиционные подходы к решению рассматриваемой проблемы заключаются в линейной компоновке алгоритмов, обнаруживающих некоторые типичные особенности шеллкодов. На практике такие подходы позволяют обнаруживать лишь отдельные виды шеллкодов. Для того, чтобы обеспечить обнаружение сразу нескольких видов, необходим запуск различных методов на одном и том же наборе данных, что на практике не осуществимо в силу слишком высокой суммарной вычислительной сложности. Даже по отдельности, применимость существующих подходов к высокоскоростным каналам остается под сомнением: методы либо сложны, либо не точны.

В данной работе ставится задача разработки метода обнаружения шеллкодов, обеспечивающего полное покрытие существующих известных образцов шеллкодов, а так же не ухудшающего долю ложных срабатываний, по сравнению с существующими решениями, и уменьшающему вычислительную сложность, по сравнению с традиционным подходом к решению этой задачи. Новизна такой постановки задачи заключается в том, что она сама по себе предполагает систематизацию предметной области, а именно построение классификации шеллкодов. В традиционных решениях, как правило, рассматривается вопрос обнаружения лишь некоторого класса шеллкодов. Таким образом, диссертационная работа Гайворонской С.А. является актуальной как в теоретическом, так и в практическом плане.

Для решения указанной проблемы в работе предложены:

1. Математическая модель, позволяющая формально описать процесс распознавания шеллкодов – отнесения образцов к одному или нескольким из заданных классов, а так же изучить свойства этого процесса.
2. Предложен новый алгоритм решения задачи распознавания шеллкодов.
3. Соискателем разработано и в достаточной степени апробировано программное обеспечение реализующее выявление известных типов шеллкодов в реальном времени.

Основная идея предлагаемого подхода нова и заключается в следующем. Для каждого класса шеллкодов выделены характерные признаки, и построены элементарные алгоритмы, их вычисляющие. В отличие от традиционных решений, как правило, использующих линейную комбинацию подмножества таких алгоритмов, в предлагаемом подходе рассматривается все множество элементарных алгоритмов, на котором введено отношение частичного порядка. Автором показано, что предложенное решение действительно обеспечивает полное покрытие известных классов объектов, не ухудшает долю ложных срабатываний по сравнению с традиционным подходом к решению этой задачи, а так же позволяет понизить вычислительную сложность процесса обнаружения по сравнению с традиционными подходами.

Работа структурирована следующим образом.

Во введении приведено неформальное описание решаемой задачи, показывается ее актуальность.

Первая глава содержит описание математической модели, приведена формальная постановка задачи. В рамках введенной модели предложен подход к решению поставленной задачи, проанализированы и доказаны его свойства.

Во второй главе соискатель описывает типичные признаки, или свойства шеллкодов, на основании которых строятся элементарные алгоритмы.

В третьей главе приведен анализ существующих решений задачи обнаружения шеллкодов. Соискателем показывается, что существующие подходы не обеспечивают полного покрытия приведенных классов шеллкодов.

В четвертой главе настоящей работы описано программное средство, реализующее предложенный подход, описана методика тестирования и приведены результаты экспериментального исследования.

Результаты работы опубликованы в ведущих научных журналах, в том числе из списка ВАК, и представлены на ведущих международных конференциях по информационной безопасности.

В качестве недочетов по содержанию и оформлению данной работы можно указать следующие:

1. Расчет оценки сложности предложенной модели алгоритма не сопровождается пояснениями и обоснованиями выбора отдельных параметров
2. Теоретическая оценка эффективности алгоритма представляется заниженной. Реальная работоспособность процедуры выявления шеллкодов существенно выше.
3. Обзор существующего состояния и методов решения задачи обнаружения шеллкодов чрезмерно детален, а вывод о недостатках известных ранее решений, можно было сделать на основе ссылок.
4. В тексте содержится ряд стилистических и пунктуационных ошибок. Не выделены блоки программного обеспечения, разработанного лично автором. Например, дизассемблер.

Отмеченные недостатки не влияют на общую высокую оценку работы. Работа производит целостное впечатление, написана на хорошем уровне, содержит четкую постановку задачи, анализ как самих шеллкодов, известных на сегодня, так и методов их обнаружения, а так же подробное описание тестовых наборов данных и методики тестирования. Результаты работы являются новыми и прошли апробацию на ведущих российских и международных конференциях. Научная достоверность и обоснованность полученных результатов подтверждаются правильной организацией и достаточным объемом экспериментов.

Автореферат отражает содержание диссертации. Тематика и содержание диссертационного исследования соответствуют специальности 05.13.11 - математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей.

Диссертационная работа Гайворонской С.А. представляет из себя законченное научное исследование, выполненное на высоком уровне на актуальную тему, содержит новые научные результаты, имеющие существенное значение для области информационной безопасности, и отвечает всем требованиям ВАК, предъявляемым к кандидатским диссертациям. Автор работы, Гайворонская Светлана Александровна, заслуживает присуждения ей ученой степени кандидата физико-математических наук по специальности 05.13.11 – «математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей».

Официальный оппонент,
зам. генерального директора
ФГУП ГНИВЦ ФНС РОССИИ
д.ф.-м.н. Баранов Александр Павлович

05.09.2014г.

Подпись Баранова А.П. заверяю
Начальник Отдела кадров [illegible] Н.М. Верещенко