ОТЗЫВ

научного руководителя на диссертацию Федотова Андрея Николаевича "Разработка метода оценки эксплуатируемости программных дефектов", представленную на соискание ученой степени кандидата технических наук по специальности 05.13.11 – математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

Диссертационная работа Федотова А.Н. посвящена разработке нового метода оценки эксплуатируемости выявленных программных дефектов. От метода требовалось учитывать ключевые особенности среды выполнения современных программ, а именно: механизмы защиты от эксплуатации, реализованные в ОС и встроенные в ПО компилятором в процессе сборки. Помимо того, разрабатываемый метод должен быть способен анализировать программы, работающие под управлением различных ОС.

Распространение компьютеров в быту и на производстве привело к тому, что злонамеренная эксплуатация ошибок способна нанести значительный ущерб как отдельным людям, так и организациям и даже целым государствам. Безопасность ПО невозможна без согласованного применения различных технологий на всех этапах жизненного цикла. Если инструменты статического анализа уже получили признание в промышленной разработке и всецело интегрировались с другими инструментами, методы фаззинга страдают от ряда недостатков. Фаззинг больших промышленных программ вырабатывает множество, в публикациях речь идет о десятках тысяч, аварийных завершений. Ручной разбор такого потока аварийных завершений невозможен, остро стоит задача выделения среди них тех, которые обусловлены эксплуатируемыми дефектами. Наибольший приоритет должны получать те дефекты, эксплуатация которых приводит к срабатыванию произвольного, внедренного извне, кода.

В научной среде вопрос автоматического построения эксплойтов активно обсуждается последние десять лет, поскольку успешное построение эксплойта позволяет безошибочно оценить критичность соответствующего программного дефекта. Но, к сожалению, известные работы оказываются неприменимы на практике в силу предельно упрощенной модели среды выполнения, защитные механизмы операционных систем и внедряемые компилятором в код программ. Все эти факторы делают работу Федотова А.Н. крайне актуальной.

В ходе работы над диссертацией Федотов А.Н. последовательно и системно решал поставленные задачи. Им была разработан архитектурно независимый метод автоматической генерации эксплойтов, позволяющих выполнять заданный аналитиком код. Входными данными для метода выступает информация об аварийном завершении

программы. Метод учитывает влияние механизмов защиты от выполнения данных (DEP) и рандомизации адресного пространства процесса (ASLR) на возможность эскалации последствий от срабатывания дефекта, что позволяет гораздо точней выявлять критичные для безопасности ПО дефекты. Метод применим к программам, работающим под управлением ОС Linux и семейства ОС Windows. Попытка построить эксплойт предваряется легковесной фильтрацией, отбрасывающей неэксплуатируемые дефекты. На базе этих двух методов (построения эксплойта и предварительной фильтрации) был разработан и реализован метод оценки эксплуатируемости программных дефектов по потоку аварийных завершений программы.

Полученные диссертантом результаты были опубликованы в авторитетных изданиях и обсуждались на конференциях.

Считаю, что диссертационная работа соответствует всем требованиям, предъявляемым ВАК к работам на соискание ученой степени кандидата технических наук по специальности 05.13.11 – математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей – а ее автор, Федотов Андрей Николаевич, заслуживает присуждения ему ученой степени кандидата технических наук по специальности 05.13.11.

Научный руководитель: в.н.с. ИСП РАН, к.ф.-м.н. В.А. Падарян

12 октября 2017 года

Подпись Падаряна В.А. удостоверяю

директор ИСП РАН Аветисян А.И.