УДК 004.052.34

РАЗРАБОТКА АНАЛИЗАТОРА ОПЕРАТИВНОЙ ПАМЯТИ С ЦЕЛЬЮ ДЕТЕКТИРОВАНИЯ ПОТЕНЦИАЛЬНЫХ УЯЗВИМОСТЕЙ

Иванов А.А. (Университет ИТМО)

Научный руководитель – кандидат технических наук, доцент Кузнецов А.Ю.
(Университет ИТМО)

Доклад посвящен проблемам детектирования уязвимостей в программном обеспечении. Предложены алгоритмы поиска потенциальных уязвимостей, на основе которых разработана программа-анализатор.

Введение. Одной из главных угроз информационной безопасности было и остается наличие в программном обеспечении уязвимостей. Во многих программных продуктах последних версий имеются еще неизвестные уязвимости из-за трудности поиска в программном коде проблемных частей: автоматизированные системы анализа программ и программных кодов (динамические и статические анализаторы, фаззеры) нацелены на поиск ошибок, но зачастую не способны отличить тривиальную ошибку от потенциальной уязвимости. В виду этого было принято решение, разработать программу-анализатор, направленную на анализ не всего программного обеспечения, а ситуаций, вызывающих внутренние ошибки, с целью обнаружения потенциальных уязвимостей и исключения тривиальных ошибок.

Основная часть. Для того, чтобы разработать программу-анализатор, необходимо определить методы, с помощью которых можно отличать потенциальные уязвимости от ошибок. Для этого была проанализирована всемирная база данных известных уязвимостей (CVE), на основе которых удалось выявить «паттерны» для каждой типовой уязвимости – определенные состояния оперативной памяти в момент возникновения внутренней ошибки в программе. Анализируя состояние программы, становится возможно искать данные «паттерны» и в случае обнаружения предупреждать о том, что найдена потенциальная уязвимость. Для программной реализации анализатора на основе выделенных «паттернов» были составлены алгоритмы поиска потенциальных уязвимостей, которые возможно использовать программно. При этом возможность проведения такого анализа программ дают специальные фреймворки динамической бинарной инструментации, один из которых был использован непосредственно при разработке программы-анализатора.

Выводы. Выделенные и сформулированные в данной работе «паттерны» потенциальных уязвимостей могут использовать разработчики программного обеспечения, для того чтобы не допускать опасных ситуаций при работе разрабатываемой программы. Разработанную программу-анализатор можно использовать как для анализа отдельно обнаруженных ошибок в программе, так и в совокупности с автоматизированными системами поиска ошибок, например, фаззерами, для выявления потенциальных уязвимостей среди всех найденных такими системами ошибок.

Иванов А.А. (автор)

Кузнецов А.Ю. (научный руководитель)