

ОТЗЫВ

на автореферат диссертации Лубкина Ивана Александровича «Метод снижения подверженности приложений к реализации уязвимостей за счет обфускации машинного кода», представленной на соискание ученой степени кандидата технических наук по специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность»

Тема диссертационной работы является актуальной для эксплуатируемых в организациях приложений, к которым имеется доступ у атакующего, вне зависимости от наличия их исходных текстов. Существующие средства защиты либо не обеспечивают надлежащего уровня защиты при наличии у атакующего возможности раскрытия содержимого памяти защищаемых программ, либо неприменимы для указанных сценариев в полном объеме. Автором рассмотрена наиболее популярная для офисного и серверного применения архитектура команд AMD64. Работа посвящена совершенствованию существующих подходов к защите для устранения недостатков, присущих существующим решениям.

В работе получены модель вычисления выходных данных программ и модель *RoP*-атак. На их основе сформированы метод снижения подверженности приложений к реализации уязвимостей за счет обфускации машинного кода и метод оценки эффективности средств защиты программ от *RoP*-атак. Это позволило сформировать алгоритмы, необходимые для программной реализации предложенного средства защиты.

Достоверность разработанных методов, методики и моделей подтверждается как успешным повышением защищенности заведомо уязвимого приложения, так и кардинальным снижением числа гаджетов в защищаемых приложениях с отсутствием из них пригодных для атак.

Важно отметить, что результаты, представленные в работе, опубликованы в различных изданиях (всего 14 публикаций): 7 статей из перечня ВАК, 3 статьи в журнале, индексируемых в базе Scopus, 4 в прочих изданиях. По теме работы получены 2 свидетельства о регистрации программ.

По мере прочтения автореферата возникли следующие вопросы и замечания:

1. При расчете метрики защищенности N_{π} в соответствии с представленным алгоритмом не ясно, учитываются ли регистры для инструкций с неявным указанием операндов (например, XLAT).

2. На странице 21 не приведены результаты метрики защищенности N_{π} , определенной для средства G-free, а лишь указано соотношение с предлагаемой реализацией.

Указанные недостатки не снижают ценности проделанной работы.

В целом, по результатам ознакомления с авторефератом можно заключить, что диссертационная работа Лубкина Ивана Александровича соответствует требованиям ВАК, предъявляемым к кандидатским диссертациям по научной новизне, практической значимости и масштабам внедрения по специальности 2.3.6 – Методы и системы защиты информации, информационная

безопасность. Автор работы достоин присвоения ученой степени кандидата технических наук.

Я, Садыков Александр Мунирович, даю свое согласие на включение моих персональных данных в документы, связанные с работой диссертационного совета, и их дальнейшую обработку.

Доцент кафедры ИБ, Федеральное государственное бюджетное образовательное учреждение высшего образования «Казанский национальный исследовательский технологический университет» (ФГБОУ ВО «КНИТУ»), к.т.н.

Электронная почта: alex.sadykov@mail.ru

Рабочий телефон: +7 (843) 231-42-16

Адрес: 420015, Российская Федерация, Республика Татарстан, Казань, ул.К.Маркса, 68,


Садыков Александр Мунирович

Подпись Садыкова Александра Мунировича заверяю _____

Подпись Садыков А.М.

_____ удостоверяю.
Начальник отдела по работе с
сотрудниками ФГБОУ ВО «КНИТУ»

« 04 » 12 А.Р. Урбанский

