Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056.53

Петухов
Алексей Владимирович

Исследование и анализ защищенности мобильных приложений на основе построения теста на проникновение

АВТОРЕФЕРАТ

на соискание степени магистра технических наук

по специальности 1-40 80 05 Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

Научный руководитель
Медведев Сергей Александрович
к.т.н., доцент

Минск 2017

КРАТКОЕ ВВЕДЕНИЕ

В настоящее время трудно представить жизнь без мобильных устройств, они стали неотъемлемой частью повседневной жизни каждого человека, выполняя все больше и больше задач. Использование мобильного гаджета предполагает хранение и передачу личной информации. В связи с этим немаловажное значение следует уделять безопасности портативных устройств и программному обеспечению. В наше время все большее количество разработчиков стремятся выпускать защищенные приложения, цель которого сохранить пользовательскую информацию от взлома и распространения третьими лицами.

Все смартфоны, как компьютеры, являются потенциальными объектами хакерских атак. Эти атаки используют слабые места, присущие смартфонам, которые могут поступать из режима режима передачи данных, например службы коротких сообщений SMS, службы мультимедийных сообщений MMS, wifi, Bluetooth и GSM, которые фактически являются глобальным стандартом для мобильной связи. Существуют также эксплойты, нацеленные на уязвимости программного обеспечения в браузере или операционной системе.

Как и множество других инновационных технологий, использование беспроводных сетей влечет не только новые выгоды, но и новые риски. Бум Wi-Fi породил целое новое поколение хакеров, специализирующихся на изобретении всё новых и новых способов взлома беспроводки и атаки пользователей и корпоративной инфраструктуры. Беспроводная связь и мобильность, которую она дает, интересны и выгодны многим. Однако, до тех пор, пока вопрос беспроводной безопасности остается не до конца ясным, мнения разнятся кардинально: некоторые (например, операторы складов) уже сейчас не боятся завязывать на Wi-Fi свои ключевые бизнес-процессы, другие – наоборот баррикадируются и запрещают использование беспроводных элементов в своих сетях.

Контрмеры безопасности разрабатываются и применяются к смартфонам и приложениям от безопасности в различных уровнях программного обеспечения до распространения информации для конечных пользователей. Существуют надежные методы, которые должны соблюдаться на всех уровнях: от

проектирования до использования, разработки операционных систем, уровней программного обеспечения и загружаемых приложений.

В результате проведения анализа существующих объектно-ориентированных моделей, методов и программных средств тестирования на проникновение для мобильных устройств в работе были выделены вышеуказанные проблемы организации тестирования на проникновение. На основе выделенных проблем сформированы общие проблемы защищености данных на мобильных устройствах – проблемы обеспечения безопасности, производительности, масштабируемости, прозрачности и отказоустойчивости. Учитывая сформированные общие проблемы, сформулирована система критериев оценки эффективности тестирования на проникновение. Сформулированная система критериев использована для анализа результатов экспериментов, проводимых с разработанным и исследованными методами, с целью проверки улучшения значений критериев оценки эффективности у разработанной модели по сравнению с исследованными. Так как в результате проведения экспериментов достигнуто улучшение значений критериев оценки эффективности у реализованной модели, то сделан вывод о том, что разработанные модели и методы тестирования предлагают более эффективные решения вышеуказанных общих проблем в области мобильной безопасности.

В качестве исходных данных для проведения исследования использовались научная литература по рассматриваемой теме, ПО для создания модели тестирования приложений, также для проведения экспериментов с исследуемыми и разработанным методами.

Таким образом, тема работы обоснована и актуальна в научном (исследование и анализ защищенности мобильных приложений на основе построения теста на проникновение) и практическом плане (эксперименты, подтверждающие улучшение значений критериев оценки эффективности метода тестирования по сравнению с исследованными методами тестирования на проникновение для мобильных устройств).

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Целью диссертационной работы является исследование и анализ защищенности мобильных приложений на основе построения теста на проникновение в недерминированных сетях, и проведения практической проверки наличия преимуществ моделей в рамках созданного сценария тестирования над уже существующими моделями.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Исследовать существующие модели, алгоритмы и программные средства теста на проникновение в недетерминированных сетях на мобильных устройствах и определения проблем тестирования.

2. Разработать методы и анализ тестирования на проникновение для мобильных устройств.

3. Разработать программное решение на основе созданных моделей и методов тестирования.

4. Провести экспериментальные исследования разработанного программного решения.

Объектом исследования являются область теста на проникновение для мобильных устройств.

Предметом исследования является моделирование и алгоритмизация теста на проникновение для мобильных устройств.

Основной *гипотезой*, положенной в основу диссертационной работы, является возможность улучшения эффективности и автоматихации тестирования на проникновение для мобильных устройств в недетерминированных сетях у разработанного метода по сравнению с существующими методами на примере тестирования мобильного приложения.

Связь работы с приоритетными направлениями научных исследований и запросами реального сектора экономики

Работа выполнялась в соответствии с научно-техническим заданием и планом работ кафедры «Программное обеспечение информационных технологий» по теме «Разработка моделей, методов, алгоритмов, повышающих показатели проектирования, внедрения и эксплуатации программных средств для перспективных платформ обработки информации, решения интеллектуальных задач, работы с большими массивами данных и внедрение в современные обучающие комплексы» (ГБ No 16-2004, No ГР 20163588, научный руководитель НИР – Н. В. Лапицкая).

Личный вклад соискателя

Результаты, приведенные в диссертации, получены соискателем лично. Вклад научного руководителя С. А. Медведев, заключается в формулировке целей и задач исследования.

Апробация результатов диссертации

Основные положения диссертационной работы докладывались и обсуждались на международной научно-практической конференции: «Фундаментальные и прикладные научные исследования» (Москва, Россия, 2017); международной научно-практической конференции: «Перспективы развития информационных технологий» (Новосибирск, Россия, 2017).

Опубликованность результатов диссертации

По теме диссертации опубликовано 2 печатные работы, из них 2 работа в системе Российского индекса научного цитирования (РИНЦ)

Структура и объем диссертации

Диссертация состоит из общей характеристики работы, введения, трех глав, заключения, списка использованных источников, списка публикаций соискателя и приложений. В первой главе представлен анализ предметной области, выявлены основные существующие проблемы в рамках тематики исследования, показаны направления их решения. Вторая глава посвящена разработке модели теста на проникновение в недетерминированных сетях. В третьей главе рассмотрена методология разработанной модели на практике и построена система критериев оценки эффективности данного способа. Проведены эксперименты по проверки улучшения значений критериев оценки работы у разработанной модели по сравнению с исследованными.

Общий объем работы составляет 65 страниц, из которых основного текста – 56 страница, 15 рисунков на 15 страницах, список использованных источников из 31 наименований на 3 страницах и 2 приложение на 2 странице.

ОСНОВНОЕ СОДЕРЖАНИЕ

Во **введении** определена область и указаны основные направления исследования, показана актуальность темы диссертационной работы, дана краткая характеристика исследуемых вопросов, обозначена практическая ценность работы.

В **первой главе** рассматриваются безопасность архитектуры мобильных платформ. Определяются существенные недостатки безопасности и необходимость и цели проведения тестов на проникновение для мобильных платформ в недетерминированных сетях и выявлены актуальные проблемы исследования.

В результате проведенного анализа систем, алгоритмов шифрования и программных средств шифрования выявлены общие проблемы - проблемы обеспечения безопасности на мобильных устройствах и сложности в обучении системы. Сформулированные задачи дальнейшего исследования: разработка моделей и методов теста на проникновение, предлагающие заблаговременное нахождение и устранение выявленных проблем в недетерминированных сетях, а также автоматизация процесса тестирования. Разработка набора решений на основе созданных моделей и методов для теста на проникновение. Построение

методологий оценки эффективности работы и выявление проблем. Проведение экспериментальных исследований с использованием методов исследования.

Вторая глава посвящена анализу методов тестирования на проникновение на основе алгоритмов Флойда Уоршелла и Дейкстры. Для нахождения максимально эффективного сценария тестирования были предложены два метода тестирования на проникновение: простой и комбинированный, что позволяет точно проверить эффективность системы. На экспериментальных машинах интерпретируются различные комбинации нападений. Выполненные атаки, а также возможные векторы атаки организованы в отдельные диаграммы подавление атаки, чтобы точно определить наиболее эффективные проблемные зоны.

Построена древовидная структура тестирования, которая позволяет расширять и автоматизировать систему тестирования.

Разработана структура теста на проникновение с возможность расширения системы.

Разработана спецификация теста на проникновение с использованием сетевой модели, а также его архитектура.

Определены цели и результаты используемых методов и моделей.

В **третьей главе** выбрана технология и среда проведения теста на проникновение.

На основе созданных моделей и методов реализован метод теста на проникновение, который включает: тест, статический анализ, динамический анализ, сетевой анализ, анализ файлов.

Выведены результаты работы теста на проникновение. Выявлены недостатки проведения тестирования - для успешного выполнения которого необходимо взломать целевое устройство.

Проведены эксперименты, в ходе которых были выявлены достоинства и недостатки разработанного метода. Экспериментально подтверждена гипотеза исследований о том, что разработанная модель является более актуальной и гибкой по сравнению с существующими. Объединение всех стадий тестирования и анализа может способствовать всестороннему тестированию и пониманию потенциального риска сети

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

Главный научный результат выполненной диссертационной работы заключается в развитии и усовершенствовании методов тестирования на проникновение для мобильных устройств, что позволяет повысить уровень безопасности всей системы и сохранности пользовательских данных, что может квалифицироваться как решение актуальной научно-технической задачи, имеющей существенное значение для развития мобильных операционных систем и существенному повышению безопасности.

К основным научным результатам, полученным при выполнении диссертационной работы, следует отнести следующие результаты:

1. В ходе исследования была разработана сетевая модель теста на проникновение в недетерминированных сетях, основанная на сочетании предложенных алгоритмов. Модель состоит из двух основных подходов: простой подход выбора и комбинированный подход, что позволяет точно проверить эффективность системы. На экспериментальных машинах интерпретируются различные комбинации нападений. Выполненные атаки, а также возможные векторы атаки организованы в отдельные диаграммы подавление атаки, чтобы точно определить наиболее эффективные проблемные зоны.

2. Выполнена программная реализация предложенной модели и методов тестирования и получены результаты анализа, согласно которым тестирование можно автоматизировать и проводить для мобильных приложений.

3. Построена древовидная структура тестирования, которая позволяет расширять и автоматизировать систему тестирования.

4. Проведены эксперименты, в ходе которых были выявлены достоинства и недостатки разработанного метода. Экспериментально подтверждена гипотеза исследований о том, что разработанная модель является более актуальной и гибкой по сравнению с существующими. Объединение всех стадий тестирования и анализа может способствовать всестороннему тестированию и пониманию потенциального риска сети.

Рекомендации по практическому использованию результатов

1. Предложенный метод, как показали результаты исследования его эффективности, обеспечивает производить цельное тестирование на проникновение в мобильных средах.

2. Разработан объектно-ориентированные сценарий тестирования, реализующие предложенную модель, обеспечивающие автоматизацию и полный анализ отчетных данных.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1. Петухов, А.В. Алгоритм обнаружения кибератаки для веб-приложений / А.В. Петухов // Международная научно-практическая конференция: фундаментальные и прикладные научные исследования. – 2017. – Москва: Издательство ЦРНС. – с. 95–99.

2. Петухов, А.В. Безопасность данных на мобильных устройствах / А.В. Петухов // Международная научно-практическая конференция: перспективы развития информационных технологий. – 2017. – Новосибирск: Издательство ЦРНС. – с. 12–19.