УДК: 004.056.5:004.85

РАЗРАБОТКА ГИБРИДНОЙ НЕЙРОСЕТЕВОЙ МОДЕЛИ НА ОСНОВЕ CODEBERT И ГРАФОВЫХ СЕТЕЙ ДЛЯ АВТОМАТИЗИРОВАННОГО ПОИСКА УЯЗВИМОСТЕЙ В ПРОГРАММНОМ КОДЕ НА ЯЗЫКЕ С

Захаров А.П. (ФГАОУ ВО СевГУ)
Научный руководитель – доцент кафедры «Информационная безопасность»
Маслова М.А. (ФГАОУ ВО СевГУ)

Введение.

В современном мире идет активная цифровизация всех областей жизни, из-за этого растет и сложность, и количество программ, а также требования к безопасности. В этих условиях проблема выявления уязвимостей на ранних этапах жизненного цикла разработки приобретает критическое значение, благодаря росту «цены уязвимости». Традиционные средства статического тестирования (SAST), опирающиеся на лексический анализ, регулярные выражения и жестко заданные эвристические правила, демонстрируют существенные ограничения [1]. Практика показывает, что классические анализаторы генерируют избыточное количество ложных срабатываний и не способны эффективно детектировать сложные логические уязвимости, эксплуатация которых зависит от неявных потоков данных и меж процедурных вызовов.

Основная часть.

Все чаще для поиска уязвимостей, прибегают к методам, основанным на искусственном интеллекте. Есть две основные ветви исследования этой области применения искусственного интеллекта. Первая ветвь исследует применение моделей на применении NLP-моделей (Natural Language Processing) [2], обрабатывающие исходный код как обычный текст, то есть последовательность токенов текста. Этот подход показывает высокую семантическую точность (могут выявить утечку памяти), но также теряют структуру и контекст исполнения программы. Вторая ветвь анализирует код программы как граф с помощью GNN (графовых нейронных сетей), которые могут не терять контекст с помощью представления кода как графа свойств кода (CPG), который в свою очередь состоит из абстрактного синтактического дерева (AST), графа потока управления (CFG), граф потока данных (DFG) и граф вызовов (CG). Однако в большинстве подобных работ узлы графа инициализируются примитивными векторами признаков, игнорирующими богатую смысловую нагрузку имен переменных и типов данных. Наличие этого разрыва формирует актуальную научную проблему: необходимость создания унифицированного метода, способного одновременно учитывать как лексико-семантические особенности программирования, так и топологию выполнения программного кода.

В связи с тем, что два метода имеют проблемы, предложено решение в рамках исследования, а именно разработана гибридная структура нейронный сети. В данном решении исходный код программы сначала переводится в грабовое преставление CPG. Тем самым сохраняется информация о зависимостях между удаленными участками программы и их взаимодействие между собой.

Для оптимального метода решения поставленной проблемы является алгоритм контекстно-зависимой инициализации вершин графа. Вместо традиционной схемы кодирования признаков (one-hot encoding или случайной инициализации), каждый фрагмент исходного кода, соответствующий узлу графа, обрабатывается пред обученной моделью архитектуры Transformer (модификация CodeBERT). Эта модель извлекает высоко размерные семантические эмбеддинги, учитывающие локальный контекст применения переменных, вызовов функций и операторов. В результате топологическая

структура обогащается векторами, отражающими смысловую нагрузку каждой микрооперации.

В итоге мы получаем граф отражающий контекст и взаимодействие различных частей кода, и узлы, представляющие собой эмбендинги CodeBERT, сохраняющий высокий уровень определения семантики кода. На следующем этапе пространственного анализа применяется многослойная графовая сеть с механизмом внимания (Graph Attention Network, GAT). Механизм многоголового внимания (multi-head attention) позволяет модели динамически вычислять значимость соседних узлов при агрегации признаков. Сеть самостоятельно «выучивает», какие именно ветвления кода или передачи параметров имеют наибольший вес для классификации состояния как уязвимого. Для обеспечения вычислительной экономичности и возможности запуска системы на аппаратном обеспечении потребительского класса (базовые графические ускорители), в архитектуру внедрены слои пакетной нормализации и применена стратегия динамического управления шагом обучения (Learning Rate Decay). Кроме того, для компенсации естественного дисбаланса классов в выборке (преобладание безопасного кода над уязвимым) на этапе вычисления функции потерь введено автоматическое пере взвешивание штрафов, что предотвращает деградацию предсказательной способности модели.

В результате модель была обучена на датасете из 27000 функций, которые были переведены в графовое представление с узлами из эмбендангов CodeBERT и обучена согласно вышеописанному методу. Гибридная нейросетевая архитектура продемонстрировала высокую скорость сходимости и превзошла изолированные текстовые и структурные анализаторы по метрикам точности и полноты. Метод успешно преодолевает проблему стагнации обучения (попадание в локальные минимумы) за счет сбалансированной передачи информации по связям графа, обеспечивая точную классификацию меж процедурных дефектов. А также стоит отметить скорость процесса всего обучения от генерации графов, очистки их, добавления эмбендингов CodeBERT.

Выводы.

В итоге можно уверенно утверждать о том, что данное решение можно интегрировать в конвейер безопасной разработки, Внедрение гибридной модели в качестве интеллектуального препроцессора позволит автоматизировать аудит коммитов, радикально снизить нагрузку на специалистов по информационной безопасности (за счет отсеивания ложных срабатываний классических SAST-инструментов) и приоритизировать реальные угрозы. Дальнейшие исследования и развитие системы, будут направленны на увеличение точности модели, добавление новых языков программирования для анализа, а также возможность интерпретации результата, не просто в оценку уязвима/безопасно, а показ какой именно элемент программы является не безопасным, и внедрения данной системы в реальные среды разработки.

Список использованных источников:

1 - Белоус, А. А., Маслова, М. А. МЕТОД СТАТИСТИЧЕСКОГО АНАЛИЗА ЛОКАЛЬНОЙ СЕТИ И ВЫЯВЛЕНИЯ АНОМАЛИЙ НА ДОВЕРИТЕЛЬНЫХ ИНТЕРВАЛАХ [Текст] / А. А. Белоус, М. А. Маслова // Современные проблемы радиоэлектроники и телекоммуникаций. — 2024. — № 7. — С. 221.

2 - Бусько, Н. А., Федорченко, Е. В., Котенко, И. В. Автоматическое оценивание эксплойтов на основе методов глубокого обучения [Текст] / Н. А. Бусько, Е. В. Федорченко, И. В. Котенко // Современные проблемы радиоэлектроники и телекоммуникаций. — 2024. — № 3 (53). — С. 408-420.