

Е. Н. Трошина, А. В. Чернов

Инструментальная среда восстановления исходного кода программы — декомпилятор TyDec

Декомпилятор — это инструмент, позволяющий восстанавливать программы из низкоуровневого представления в высокоуровневое. В данной работе к декомпиляции помимо корректного восстановления программ выдвигается дополнительное требование — «качественное восстановление». Инструментальное средство восстановления программ — декомпилятор TyDec, разработанный авторами данной статьи — восстанавливает программы в низкоуровневом представлении и дизассемблированные трассы программ в программы на языке Си корректно и качественно.

Введение

Создание и разработка сложных программных систем различного назначения часто ведется посредством интеграции отдельных компонент, выполненных как собственными, так и сторонними разработчиками. Это позволяет значительно сократить стоимость и время разработки программного обеспечения. При этом внешние модули могут поставляться без исходного кода. Наличие таких модулей в системе снижает уровень надежности разрабатываемого приложения с точки зрения информационной безопасности. В частности, сторонние модули могут содержать закладки или уязвимости, способствующие утечке информации и успешным атакам на информационную систему. Кроме того, программные модули от внешних разработчиков могут содержать ошибки, исправление которых оказывается затруднительным. Следовательно, весь сторонний код должен подвергаться аудиту с точки зрения безопасности его внедрения и использования.

Программные компоненты, представленные в виде исполняемых файлов или на языке ассемблера, сложны для анализа специалистами в области информационной безопасности. Для более качественного

и продуктивного анализа лучше иметь их представление на языке более высокого уровня, в частности на языке программирования Си. Ассемблерный код и, тем более, исполняемые файлы не позволяют с приемлемыми трудозатратами оценить взаимосвязь элементов программы, а также идентифицировать различные алгоритмические конструкции, в то время как наличие восстановленной программы на языке высокого уровня дает возможность преодолеть указанные выше трудности. В качестве одного из средств для повышения уровня абстракции представления программы может использоваться декомпиляция.

Декомпиляция — это процесс автоматического восстановления программы из низкоуровневого представления в высокоуровневое. Под декомпилятором будем понимать инструментальное средство, получающее на вход программу на языке ассемблера или другое аналогичное представление, и выдающее на выход эквивалентную ей программу на некотором языке высокого уровня.

Также декомпиляция может использоваться для обеспечения совместимости программных приложений, а именно для анализа протоколов взаимодействия в случае, когда они описаны недостаточно полно или