УДК 004.056

РАЗРАБОТКА АЛГОРИТМА ЗАЩИТЫ ИСПОЛНЯЕМЫХ ФАЙЛОВ ОТ ОТЛАДКИ В ОПЕРАЦИОННОЙ СИСТЕМЕ LINUX

Дронов В.Ю. (Университет ИТМО)
Научный руководитель – кандидат технических наук, доцент Гирик А.В.
(Университет ИТМО)

Введение. Злоумышленник, используя специализированные средства, способен в ходе анализа исполняемых файлов раскрыть информацию о функциональности и принципах работы программного обеспечения, обнаружить и проэксплуатировать найденные уязвимости, модифицировать программу с целью получения какого-либо преимущества. Одним из таких средств являются отладчики, позволяющие пошагово исследовать работу программы. Для повышения защищённости программных продуктов от использования уязвимостей и ошибок кода, исключения или снижения финансовых и репутационных рисков вследствие утечки или кражи оригинальных разработок появляется необходимость в разработке эффективного программного средства, осуществляющего защиту программного обеспечения от отладки. В данной работе рассматриваются существующие методы защиты исполняемых файлов от отладки и выбираются наиболее эффективные для реализации разрабатываемого алгоритма. [1]

Основная часть. Существуют различные обстоятельства, влияющие на выбор методов для защиты программного кода. В связи с этим в данной работе рассматривается применение методов защиты исполняемых файлов от отладки в следующих случаях:

1) При наличии текстов исходного кода исполняемых файлов.
2) При отсутствии текстов исходного кода (в наличии только сами исполняемые файлы).

Среди методов защиты от отладки рассматриваются такие, как применение специализированных системных вызовов, временной анализ, обнаружение процессов, проверка статуса, обнаружение точек останова и другие [2]. Также изучаются и применяются наиболее эффективные методы их реализации, позволяющие затруднить как обнаружение мер защиты злоумышленником, так и их преодоление. В ходе работы предлагается разработка алгоритма для программного средства, применяющего известные методы для защиты кода от отладки. Программное средство внедряет в код целевой программы участки кода и функции, реализующие данные методы. Целевые программы представляют собой файлы формата ELF в системе Linux.

Выводы. В результате проделанной работы были рассмотрены известные методы защиты исполняемых файлов от отладки, а также выбраны наиболее эффективные из них. На основании особенностей проанализированных методов было предложено программное решение, которое позволяет повысить защищённость программных продуктов от отладки.

Список использованных источников:

1. Красов А.В., Зуев И.П., Карельский П.В., Радынская В.Е., Гераськина В.С. Алгоритмы и методы защиты программного кода на базе обфускации // Журнал i-methods. – 2020. – № 12(1).
2. Schallner M. Beginners guide to basic linux anti anti debugging techniques // Code Breakers Magazine. – 2006. – Т. 1.

Дронов В.Ю. (автор) Подпись

Гирик А.В. (научный руководитель) Подпись