МЕТОДЫ ОБФУСКАЦИИ ПРОГРАММНЫХ СРЕДСТВ С ЦЕЛЬЮ ЗАЩИТЫ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Водейко А.Э.

Ярмолик В.Н. – д.т.н.,профессор

На сегодняшний день широко используются технологии разработки ПО, сильно уязвимые к обратному проектированию. В первую очередь, эта проблема касается таких языков программирования, как Java, C#. Для затруднения обратного проектирования используется метод, называемый обфускацией, который не изменяет функциональность программы, но усложняет анализ и понимание алгоритмов работы программы и усложняет модификацию.

Обфускация состоит в отображении исходной программы P={..., Sj, ...}, состоящей из исходного объекта Sj, в новую программу P*=={..., Ti(Sj), ...} на основании эквивалентных преобразований Ti [1]. Сама по себе обфускация не позволяет пресечь попытки несанкционированного доступа к программе, так как не изменяет функциональность программы, поэтому её применяют с другими методами защиты. Целью обфускации является затруднение, а в идеале - предотвращение таких атак, как обратное проектирование и модификация программы. Различают следующие уровни обфускации, характеризующиеся целью, объёмом и сложностью преобразований кода: лексическая обфускация, обфускация потока выполнения, обфускация данных[2].

Наиболее простой является лексическая обфускация. Она заключается в снижении читабельности исходных кодов программного средства. Это достигается за счёт следующих действий:

– добавления лишних, изменение или удаление комментариев;

– нестандартного форматирования;

– переименование идентификаторов так, чтобы их названия не отражали их предназначения и трудно воспринимались человеком.

Такой метод имеет низкую эффективность, так как не изменяется схема работы программы и практически полностью восстанавливаются при автоматической деобфускации.

Обфускация данных использует реструктуризацию данных в изменении представления данных. Она осуществляется путём объединения нескольких массивов в один, или, наоборот, разделение одного массива на несколько отдельных переменных, использования одной переменной большей разрядности для хранения нескольких переменных меньшей разрядности, изменение количества измерений массива, расщепления переменных и т.д.

Обфускация потока выполнения заключается в преобразовании графа передачи управления программы.

Большинство алгоритмов преобразования управления используют понятие “непрозрачный

предикат". Непрозрачным предикатом называют выражение, результат которого известен обфускатору, но является трудно определимым для деобфускатора. Непрозрачные предикаты делятся на три группы[3]:

– предикат, значение которого всегда "истина". Обозначается PT.

– предикат, значение которого всегда "ложь". Обозначается PF.

– предикат, значение которого зависит от некоторых условий. Обозначается P?.

С помощью трёх разновидностей предикатов можно выполнить преобразования, модифицирующие передачу управления в программе.

Для определения эффективности обфускации существуют две группы методов: аналитические и эмпирические[4]. Аналитические методы основываются на критериях устойчивости, эластичности и стоимости преобразования.

Устойчивость характеризует степень сложности обратного проектирования обфусцированного кода. Эластичность – степень защиты обфусцированного кода от использования программ-деобфускаторов. Стоимость преобразования показывает, насколько увеличилось потребление системных ресурсов после осуществления процесса обфускации. Аналитические методы подходят для сравнения разных алгоритмов обфускации, но не отвечают на вопрос, какой из алгоритмов подходит лучше всего к определённому коду.

Эмпирические методы основываются на статистических данных исследований применения разных алгоритмов и позволяет выяснить, какой алгоритм будет более эффективным для определённого кода. Таким образом, обфускация является важным методом защиты программного обеспечения от обратного проектирования, однако данные методы не получили широкого распространения на данный момент.

Список использованных источников:

1. 1. Криптография, стеганография и охрана авторского права / В.Н.Ярмолик, С.С. Портянко, С.В.Ярмолик / Издательский центр БГУ – Минск, 2007. – С. 190195

2. On the (Im)possibility of Obfuscating Programs / B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. Vadhan, K. Yang. - LNCS, 2010. - P. 1-18.

3. An approach to the obfuscation of control-flow of sequential computer program / S. Chow, Y. Gu, H. Johnson, V. Zakharov - LNCS, 2001. - P. 144-155.

4. Candidate indistinguishability obfuscation and functional encryption for all circuits / Garg S., Gentry C., Halevi S., Raykova M., Sahai A., and Waters B. FOCS, 2013 - P. 22-23 5. On best-possible obfuscation / Goldwasser S., and Guy N. R. - TCC, 2007.