# *Практическая работа № 19*

**Организация защиты кода от анализа**

Цель работы: изучение опыта организации защиты кода от анализа

Теоретическое обоснование

Большинство атак защищенных компьютерных систем начинается с анализа программной реализации защитных функций системы. До тех пор пока нарушитель не проведет достаточно полный анализ программной реализации защиты, нарушитель не сможет использовать для преодоления защиты программные уязвимости атакованной системы. Поскольку уязвимости программного обеспечения, как правило, являются наиболее удобными «входными воротами» в атакуемую систему, большинство хакеров рассматривают анализ программной реализации атакуемой системы как неотъемлемый этап ее излома. Данный этап может быть пропущен лишь в том случае, если атакуемая система является типовой, и для класса систем, к которому она принадлежит, уже известны уязвимости, позволяющие преодолевать их защиту.

Кроме того, анализ программных реализаций может применяться программистами для того, чтобы выявить в коде программы, разработанной конкурирующей фирмой, интересные находки, которые в дальнейшем можно использовать в своих программах. Как правило, новая технология, разработанная специалистами одной фирмы, очень быстро осваивается конкурентами и не последнюю роль в данном процессе играет анализ программной реализации новой технологии.

Исходя из изложенного выше, у разработчиков программной системы защиты информации часто возникает естественное желание затруднить анализ разрабатываемой системы потенциальным нарушителем.

За последние 20 — 30 лет в данной области было проведено множество исследований, в результате которых был разработан целый ряд средств и методов, позволяющих увеличить трудоемкость анализа защищаемой программы в десятки раз.

Сейчас защита от анализа включается в программы довольно редко, в основном в следующие виды программного обеспечения:

* программы, оснащенные защитой от несанкционированного копирования, — обычно очень дорогие программы либо программы, предназначенные для обработки строго конфиденциальной информации;
* программные закладки, в том числе и компьютерные вирусы.

Пожалуй, самым известным примером чрезмерного увлечения разработчиков программного обеспечения защитой от анализа являются системы защиты от копирования, разработанные компанией StarForce.

На сегодняшний день существует несколько методов защиты программного кода:

–      обфускация – внесение запутывающих преобразований в исходные коды программ, написанных на языках высокого уровня;

–      шифрование – криптографическое закрытие защищаемого кода на том или ином этапе эксплуатации системы;

–      антиотладка – защита кода от средств отладки и исследования;

–      полиморфизм – генерация различных версий бинарного кода одного алгоритма; чаще всего технологию полиморфизма для защиты бинарного кода используют компьютерные вирусы, чтобы защитить собственный код; для исследования таких объектов, как правило, используются специально разрабатываемые для каждого кода алгоритмы анализа.

Существуют специальные программные средства StarFuck и StarForce Nightmare, отключающие защиту от копирования StarForce. Известны и методы обхода некоторых систем StarForce, не использующие специально разработанное программное обеспечение, а использующие лишь широко распространенные программные продукты Alcohol 120 % и Daemon Tools

Методические указания

Для выполнения практической работы вам понадобиться материал с сайтов:

Разработка ПО: защита от промышленного шпионажа — <http://www.copyprotection.ru/press/articles/?news=2772>

Анализ кода и технологии защиты — <http://www.itsec.ru/articles2/crypto/analiz-koda-i-tehnologii-zaschity/>

Анализ проблем защиты от внешнего нарушителя — <http://www.securitylab.ru/analytics/397848.php>

Анализ рынка средств защиты от копирования и взлома программных средств — <http://citforum.ru/security/articles/analis/>

Задания

* Повторите теоретический материал
* Посетите предложенные сайты
* Проведите исследование средств защиты от копирования программных продуктов
* Составьте инструкцию для системного администратора, программиста и/или разработчика программных продуктов по осуществлению защиты кода от анализа

Контрольные вопросы

1. В чём заключается анализ кода и как это может навредить?
2. Какие способы существуют для защиты от анализа кода?
3. Какие средства существуют для защиты от анализа кода?

Форма отчёта

Конспект, проверка письменной работы, ответы на вопросы