УВАЖАЕМЫЕ СТУДЕНТЫ! Изучите приведенную лекцию, законспектируйте основные сведения о методах защиты программных продуктов, проанализируйте положительные и отрицательные факторы различных методов защиты программных продуктов.

Ответы на вопросы, фотоотчет, предоставить преподавателю на e-mail: r.bigangel@gmail.com до 27.02.2023.

При возникновении вопросов по приведенному материалу обращаться по следующему номеру телефона: (072)111-37-59, (Viber, WhatsApp), vk.com: https://vk.com/daykini

ВНИМАНИЕ!!! При отправке работы, не забывайте указывать ФИО студента, наименование дисциплины, дата проведения занятия (по расписанию).

Лекция 40

Тема: Основные сведения о защите программных продуктов.

Цель: Изучить основные сведения о защите программных продуктов.

Необходимость использования систем защиты (СЗ) ПО обусловлена рядом проблем, среди которых следует выделить: незаконное использование алгоритмов, являющихся интеллектуальной собственностью автора, при написании аналогов продукта (промышленный шпионаж); несанкционированное использование ПО (кража и копирование); несанкционированная модификация ПО с целью внедрения программных злоупотреблений; незаконное распространение и сбыт ПО (пиратство).

Системы защиты ПО по методу установки можно подразделить на **системы, устанавливаемые на скомпилированные модули ПО**; **системы, встраиваемые в исходный код ПО до компиляции**; **и комбинированные**. (Envelope(virus type), API)

По используемым механизмам защиты СЗ можно классифицировать на: **системы, использующие сложные логические механизмы; системы, использующие шифрование защищаемого ПО; и комбинированные системы**. Системы первого типа используют различные методы и приёмы, ориентированные на затруднение дизассемблирования, отладки и анализа

алгоритма СЗ и защищаемого ПО. Этот тип СЗ наименее стоек к атакам, так как для преодоления защиты достаточно проанализировать логику процедур проверки и должным образом их модифицировать. Более стойкими являются системы второго типа. Для дезактивации таких защит необходимо определение ключа дешифрации ПО. Для защиты ПО используется ряд методов, таких как:

1. **Алгоритмы запутывания** - используются хаотические переходы в разные части кода, внедрение ложных процедур - "пустышек", холостые циклы, искажение количества реальных параметров процедур ПО, разброс участков кода по разным областям ОЗУ и т.п. (метод «спагетти»)

2. **Алгоритмы мутации** - создаются таблицы соответствия операндов - синонимов и замена их друг на друга при каждом запуске программы по определенной схеме или случайным образом, случайные изменения структуры программы.

```
mov op1,op2 =  push op2
               pop  op1
jmp addr    =  push addr
               ret
call addr   =  push m
               jmp addr
               m:  . . .
```

3. **Алгоритмы компрессии данных** - программа упаковывается, а затем распаковывается по мере выполнения. PKLTE, EXEPACK, zLib.

4. **Алгоритмы шифрования данных** - программа шифруется, а затем расшифровывается по мере выполнения. (Полная – частичная расшифровка)

5. **Методы затруднения дизассемблирования** - используются различные приемы, направленные на предотвращение дизассемблирования в пакетном режиме.(IDA Scripts)

6. **Методы затруднения отладки** - используются различные приемы, направленные на усложнение отладки программы. (Завешивание отладчика – обнаружение отладчика)
7. **Эмуляция процессоров и операционных систем** - создается виртуальный процессор и/или операционная система (не обязательно реально существующие) и программа-переводчик из системы команд IBM в систему команд созданного процессора или ОС, после такого перевода ПО может выполняться только при помощи эмулятора, что резко затрудняет исследование алгоритма ПО.
8. **Нестандартные методы работы с аппаратным обеспечением** - модули системы защиты обращаются к аппаратуре ЭВМ, минуя процедуры операционной системы, и используют малоизвестные или недокументированные её возможности.

По принципу функционирования СЗ можно подразделить на **упаковщики / шифраторы; СЗ от несанкционированного копирования и СЗ от несанкционированного доступа (НСД).**

Упаковщики/шифраторы

Первоначально, использовались для уменьшения объема исполняемого модуля на диске, но позднее на первый план вышла цель защиты ПО от анализа его алгоритмов и несанкционированной модификации. Для этих целей используются алгоритмы компрессии данных; приёмы, связанные с использованием недокументированных особенностей операционных систем (ОС), криптографические методы, алгоритмы мутации, запутывание логики программы.

Отрицательные стороны:

1. Замедляют выполнение кода ПО.
2. Шифрование / упаковка кода ПО вызывает затруднения при обновлении (update) и исправлении ошибок (bugfix, servicepack).
3. Данный класс систем уязвим, так как программный код, в конечном итоге, распаковывается или расшифровывается для выполнения.

4. Упаковка и шифрование исполняемого кода вступает в конфликт с запрещением самомодифицирующегося кода в современных ОС.

СЗ от несанкционированного копирования

СЗ от несанкционированного копирования осуществляют "привязку" ПО к дистрибутивному носителю (гибкий диск, CD ...). При этом на физическом уровне создаётся дистрибутивный носитель, обладающий неповторимыми свойствами (нестандартной разметкой носителя, записи на него дополнительной информации - паролей или меток), а на программном уровне создаётся модуль, настроенный на аутентификацию носителя по его уникальным свойствам. При этом возможно применение приёмов, используемых упаковщиками/шифраторами.

Положительные факторы:

1. Затруднение нелегального копирования и распространения ПО;
2. Защита прав пользователя на приобретённое ПО.

Отрицательные факторы:

1. Большая трудоёмкость реализации системы защиты;
2. Затруднение продаж из-за необходимости физической передачи дистрибутивного носителя;
3. Снижение отказоустойчивости ПО;
4. На время работы ПО занимается накопитель;

СЗ от НСД

СЗ от НСД осуществляют предварительную или периодическую аутентификацию пользователя ПО или его компьютерной системы путём запроса дополнительной информации. К этому типу СЗ можно отнести системы парольной защиты ПО, системы "привязки" ПО к компьютеру пользователя, системы с "ключевыми дисками" и аппаратно-программные системы с электронными ключами.

Парольные защиты.

Осуществляют аутентификацию пользователя ПО путём запроса дополнительных данных, имя, пароль, серийный номер. Эта информация запрашивается в

различных ситуациях, например, при старте программы, по истечении срока бесплатного использования ПО, при вызове процедуры регистрации либо в процессе установки на ПК пользователя. Такие системы очень просты в реализации и большинство парольных СЗПО использует логические механизмы, сводящиеся к проверке правильности пароля / кода и запуске или не запуске ПО, в зависимости от результатов проверки. Слабым звеном парольных защит является блок проверки правильности введённого пароля / кода, и если СЗПО не использует шифрования, достаточно принудительно изменить логику проверки для получения беспрепятственного доступа к ПО. Jz->Jmp

Системы "привязки" ПО

Системы этого типа при установке ПО на ПК пользователя осуществляют поиск уникальных признаков компьютерной системы либо сами устанавливают такие признаки. После этого модуль защиты в самом ПО настраивается на поиск и идентификацию данных признаков, по которым в дальнейшем определяется авторизованное или неавторизованное использование ПО. При этом возможно применение методик оценки скоростных и иных показателей процессора, параметров материнской платы, версий BIOS, ОС, запись скрытых файлов, реестр Windows. (скрытые места :ms, Filemon, Regmon)

Отрицательные факторы:

1. Ложные срабатывания СЗПО при любых изменениях в параметрах ПК.
2. Низкая стойкость при доступе злоумышленника к ПК пользователя.
3. Возможность конфликтов с системным ПО.

Программно-аппаратные средства защиты ПО с электронными ключами

Этот вид защиты, основан на использовании так называемых "аппаратных (электронных) ключей". Электронный ключ - это аппаратная часть системы защиты, представляющая собой плату с микросхемами памяти либо с микропроцессором, помещенную в корпус и предназначенную для установки в один из стандартных портов ПК (COM, LPT, PCMCIA, USB ...) или слот расширения материнской платы. Так же в качестве такого устройства могут

использоваться SMART-карты. Программно-аппаратные средства защиты в настоящий момент являются одними из самых стойких систем защиты ПО от НСД.

Электронные ключи по архитектуре можно подразделить на **ключи с памятью** (без микропроцессора) и **ключи с микропроцессором** (и памятью).

Ключи с памятью являются менее стойкими, в таких системах критическая информация (ключ дешифрации, таблица переходов) хранится в памяти электронного ключа. Для дезактивации таких защит в большинстве случаев необходимо наличие у злоумышленника аппаратной части системы защиты (перехват диалога между программной и аппаратной частями для доступа к критической информации), либо снятие логической защиты.

Самыми стойкими являются системы с микропроцессором. Такие комплексы содержат в аппаратной части не только ключ дешифрации, но и блоки шифрации/дешифрации данных, при работе защиты в электронный ключ передаются блоки зашифрованной информации, и принимаются оттуда расшифрованные данные. Так как все процедуры выполняются аппаратной частью, достаточно сложно перехватить ключ дешифрации.

Положительные факторы:

1. Значительное затруднение нелегального распространения и использования ПО;
2. Избавление производителя ПО от разработки собственной системы защиты;
3. Высокая автоматизация процесса защиты ПО;

Отрицательные факторы:

1. Дополнительные затраты на приобретение системы защиты и обучение персонала;
2. Замедление продаж из-за необходимости физической передачи аппаратной части;
3. Повышение системных требований из-за защиты (совместимость, драйверы);
4. Несовместимость защиты и аппаратуры пользователя;
5. Затруднения использования защищенного ПО в мобильных ПК;