ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ОТ НЕСАНКЦИОНИРОВАННОГО КОПИРОВАНИЯ

ст.гр. ВМКС 1-10 Айтбеков Р., рук. Исраилова Н.А.
КГТУ им.И.Раззакова
E-mail: rustam.aytbekoff@gmail.com

В настоящее время разработано достаточно много средств защиты программного обеспечения: программные, технические, правовые и т.д. Однако реально существует проблема выбора наиболее эффективных методов и средств защиты ПО в конкретных ИС.В данной работе предпринята попытка выявить комплекс наиболее эффективных средств и методов защиты программного обеспечения от всевозможных дестабилизирующих факторов.

Локальная программная защита. Требование ввода серийного номера (ключа) при установке/запуске. История этого метода началась тогда, когда приложения распространялись только на физических носителях (к примеру, компакт-дисках). На коробке с диском был напечатан серийный номер, подходящий только к данной копии программы.
С распространением сетей очевидным недостатком стала проблема распространения образов дисков и серийных номеров по сети. Поэтому в настоящий момент метод используется только в совокупности одним или более других методов (к примеру, организационных).

Сетевая программная защита

- локальная

Сканирование сети исключает одновременный запуск двух программ с одним регистрационным ключом на двух компьютерах в пределах одной локальной сети.
Недостаток в том, что брандмауэр можно настроить так, чтобы он не пропускал пакеты, принадлежащие защищённой программе. Правда, настройка брандмауэра требует некоторых пользовательских навыков. Кроме того, приложения могут взаимодействовать по сети (к примеру, при организации сетевой игры). В этом случае брандмауэр должен пропускать такой трафик.

- глобальная

Если программа работает с каким-то централизованным сервером и без него бесполезна (например, сервера онлайн-игр, серверы обновлений антивирусов). Она может передавать серверу свой серийный номер; если номер неправильный, сервер отказывает в услуге. Недостаток в том, что, существует возможность создать сервер, который не делает такой проверки. Например, существовал сервер *battle.da*, который по функциям был аналогичен Battle.net, но пускал пользователей неавторизованных копий игр. Сейчас этот сервер закрыт, но существует немалое количество PvPGN-серверов, которые также не проверяют регистрационные номера.

Защита при помощи компакт-дисков
Программа может требовать оригинальный компакт-диск. В частности, такой способ применяется в играх. Стойкость таких защит невелика, ввиду широкого набора инструментов снятия образов компакт-дисков.[1]
Как правило, этот способ защиты применяется для защиты программ, записанных на этом же компакт-диске, являющимся одновременно ключевым.

Для защиты от копирования используется:

- запись информации в неиспользуемых секторах;
- проверка расположения и содержимого «сбойных» секторов;
- проверка скорости чтения отдельных секторов.

Защита при помощи электронных ключей
Электронный ключ (донгл), вставленный в один из портов компьютера (с интерфейсом USB, LPT или COM) содержит ключевые данные, называемые также лицензией, записанные в него разработчиком защищенной программы. Защита программы основывается на том, что только ему (разработчику) известен полный алгоритм работы ключа. Типы ключевых данных:

- информация для чтения/записи (в настоящий момент практически не применяется, так как после считывания ключ может быть с эмулирован)
- ключи аппаратных криптографических алгоритмов (используется наиболее часто)
- алгоритмы, созданные разработчиком программы (ставший доступным сравнительно недавно метод, в связи с появлением электронных ключей с микропроцессором, способным исполнять произвольный код; в настоящее время используется все чаще)

Достоинства защиты с использованием электронных ключей:

- Ключ можно вставлять в любой компьютер, на котором необходимо запустить программу
- Ключ не занимает/не требует наличия дисковода
- Электронный ключ умеет выполнять криптографические преобразования
- Современные ключи могут исполнять произвольный код, помещаемый в них разработчиком защиты (пример — Guardant Code, Senselock)

Стойкость защиты основывается на том, что ключевая информация защиты (криптографические ключи, загружаемый код) не покидает ключа в процессе работы с ним.

Основные недостатки:

- Цена (15—30 долларов за штуку)
- Необходимость доставки ключа конечному пользователю

Ранее к недостаткам можно было также отнести невысокое быстродействие ключа (в сравнении с CPU компьютера). Однако современные ключи достигают производительности в 1.25 DMIPS (пример — HASP,Guardant), а техника защиты с их помощью не предполагает постоянного обмена с ключом.
Существовавшие также ранее проблемы с установкой ключа на определенные аппаратные платформы в настоящий момент решена при помощи сетевых ключей (которые способны работать с

одной или более копиями защищенного приложения, просто находясь с ним в одной локальной сети) и с помощью программных или аппаратных средств «проброса» USB-устройств по сети.

Привязка к параметрам компьютера и активация

Привязка к информации о пользователе / серийным номерам компонентов его компьютера и последующая *активация программного обеспечения* в настоящий момент используется достаточно широко (пример: ОС Windows).

В процессе установки программа подсчитывает код активации — контрольное значение, однозначно соответствующее установленным комплектующим компьютера и параметрам установленной ОС. Это значение передается разработчику программы. На его основе разработчик генерирует ключ активации, подходящий для активации приложения только на указанной машине (копирование установленных исполняемых файлов на другой компьютер приведет к неработоспособности программы).

Достоинство в том, что не требуется никакого специфического аппаратного обеспечения, и программу можно распространять посредством цифровой дистрибуции (по Интернет).

Основной недостаток: если пользователь производит модернизацию компьютера (в случае привязки к железу), защита отказывает. Авторы многих программ в подобных случаях готовы дать новый регистрационный код. Например, Microsoft в Windows XP разрешает раз в 120 дней генерировать новый регистрационный код (но в исключительных случаях, позвонив в службу активации, можно получить новый код и после окончания этого срока).

В качестве привязки используются, в основном, серийный номер BIOS материнской платы, серийный номер винчестера. В целях сокрытия от пользователя данные о защите могут располагаться в неразмеченной области жесткого диска.

Недостатки технических методов защиты ПО

Уязвимости современных методов защиты ПО

Уязвимости современных методов защиты можно достаточно строго классифицировать в зависимости от использованного метода защиты.

- Проверка оригинального носителя. Можно обойти при помощи копирования / эмуляции диска (специальная программа полностью копирует диск, затем создается драйвер виртуального дисковода, в который помещается образ, который программа принимает за лицензионный диск. Во многих играх применяется вариант этого метода под названием «Mini Image», когда подставной диск имеет маленький размер (несколько мегабайт, содержащие только лицензионную информацию), программа признаёт его лицензионным
- Ввод серийного номера. Основной уязвимостью является возможность беспрепятственного копирования и распространения дистрибутива вместе с серийным номером. Поэтому в настоящее время практически не используется (либо используется в совокупности с другими методами).
- Активация программного обеспечения. В отличие от предыдущего метода, активационный код генерируется с использованием уникальной информации (S/N оборудования, информации о пользователе) и является уникальным. В этом случае, в момент генерации кода активации в процессе установки программы есть риск эмуляции «универсального» аппаратного окружения (как то перехват обращений программы при считывании соответствующей информации, либо запуск программы изначально в виртуальной среде).
- «Отключение» защиты путем модификации программного кода (к примеру, удаления проверок лицензии). Может быть реализовано при неиспользовании (или использовании слабых) инструментов запутывания кода. В результате программа дизассемблируется (или даже декомпилируется, в худшем случае), код исследуется на наличие защитных механизмов, найденные проверки удаляются.

Многие защиты предоставляют инструменты противодействия взлому: дестабилизация отладчика; шифрование кода, исключающее изучение кода в статике при помощи дизассемблера; запутывание кода, «ложные ветви», сбивающие хакера с толку; проверка целостности файла, не дающая накладывать патчи; виртуализация кода с собственной системой команд. Все эти методы препятствуют изучению и анализу логики защиты, повышают её стойкость.

Вывод:

За последние 30 лет появлялись и погибали различные технологии. И сейчас многим кажется, что с развитием Интернета и цифровой дистрибуции право на существование имеет только онлайн-активация для защиты от копирования и обфускация кода для защиты от реверсинга. Однако есть и противоположная тенденция – развитие рынка SaaS и переход приложений в "облако". Если считать эту тенденцию потенциальным победителем, то защита вообще никому не нужна, ведь приложение не распространяется. Для "облаков" важна аутентификация, безопасность передачи данных и доступность сети.

Выбирая защиту для своего программного продукта, необходимо учитывать множество факторов: каналы дистрибуции (физические или цифровые), стоимость защиты, требования к надеж-

ности и отказоустойчивости. В некоторых случаях приложению вполне допустимо "уйти в облако", где защита осуществляется организационными мерами, но уже не обойтись без надежной аутентификации. Если же софт распространяется вместе с оборудованием (например, кассовые аппараты, терминалы и т.д.), то электронный ключ – это лучший и практически единственный вариант защиты. Электронные ключи (особенно с загружаемым кодом) незаменимы при защите особо ценного ПО с уникальными ноу-хау. Если приложение стоит десятки тысяч долларов, то экономить на защите не стоит, да и проблема физического распространения не столь актуальна – такое ПО зачастую внедряется армией консультантов и всегда есть "физический" контакт с клиентом.

В остальных же случаях для тиражного и недорогого софта технология онлайн-активации – это наиболее современное, надежное и относительно недорогое средство защиты. Исключением является ситуация, когда продажи осуществляются через партнерскую сеть. Софтверные лицензии не так хорошо защищают от мошенничества со стороны партнеров, электронные ключи же решают эту проблему полностью. Нельзя одну и ту же "железку" дать двум разным клиентам.

Литература

1. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. Под ред. В.Ф. Шаньгина. - 2-е изд., перераб. и доп. - М.:Радио и связь, 2001. - 376 с.: ил.
2. Андрей Щеглов, Защита компьютерной информации от несанкционированного доступа, Наука и техника, 2004 г.