УДК 004.056.52

АНАЛИЗ МЕТОДОВ ЗАЩИТЫ ПРИЛОЖЕНИЙ ОТ НЕСАНКЦИОНИРОВАННОГО ИСПОЛЬЗОВАНИЯ

А.Г. АНДРЕЙЧИКОВ
(***Представлено: канд. физ.-мат. наук, доц. Д.Ф. ПАСТУХОВ***)

В статье проведён анализ методов защиты программного обеспечения от несанкционированного использования. Рассмотрена задача реализация надёжной системы защиты критически важного программного продукта.

На сегодняшний день, любое программное обеспечение, работающее с пользовательскими данными должно быть защищённо от несанкционированного использования. Приложение, а также информация, обрабатываемая в приложении должны быть защищены. Существуют программные продукты, получение возможного доступа к которым может нанести существенные финансовые убытки или допустить утечку данных пользователей. Утечка данных пользователей может дать предполагаемому злоумышленнику данные для последующей кражи финансовых средств данного пользователя.

Защита программного обеспечения — комплекс мер, направленных на защиту программного обеспечения от несанкционированного приобретения, использования, распространения, модифицирования, изучения и воссоздания аналогов.

Защита от несанкционированного использования программ — система мер, направленных на противодействие нелегальному использованию программного обеспечения. При защите могут применяться организационные, юридические, программные и программно-аппаратные средства.

Защита от копирования к программному обеспечению применяется редко, в связи с необходимостью его распространения и установки на компьютеры пользователей. Однако, от копирования может защищаться лицензия на приложение (при распространении на физическом носителе) или его отдельные алгоритмы. [1]

Методы можно классифицировать по способу распространения защищаемого программного обеспечения и типу носителя лицензии.

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. Недостаток данного метода в простоте обхода защиты - можно беспрепятственно передавать серийный номер, а компакт-диск эмулировать. Как метод защиты в текущих реалиях практически бесполезен, но может использоваться в совокупности с другими методами защиты.

Сетевая программная защита. Локальная разновидность защиты предполагает сканирование сети что исключает одновременный запуск двух программ с одним регистрационным ключом на двух компьютерах в пределах одной локальной сети. Данный метод можно обойти, имея небольшие знания настройки брандмауэра. Если заблокировать программе доступ к локальной сети или отфильтровать исходящие пакеты можно избежать блокировки. Глобальная разновидность защиты использует централизованный сервер для контроля доступа проверяя на этапе соединения регистрационный ключ или другую информацию исключающую неавторизированный доступ. Метод обхода данного метода защиты заключается в развертывании поддельного сервера, исключающего авторизацию или авторизующей по любым пользователеям. Таким образом, получив копию оригинального сервера можно полностью проигнорировать защиту и получить доступ к программному продукту.

Защита при помощи электронных ключей. Электронный ключ — вставленный в один из портов компьютера (с интерфейсом USB, LPT или COM) содержит ключевые данные, называемые также лицензией, записанные в него разработчиком. В настоящие время из-за сложности похищения данного ключа является хорошим методом защиты при условии, что используется самый современный вариант ключа, и он защищён от посторонних лиц.

Защита программ от копирования путём переноса их в сеть Интернет. Стремительно набирающий популярность метод защиты, который заключается в предоставление функционала программ (всего или части), как сервиса онлайн, в сети Интернет. При этом код программы расположен и исполняется на сервере, доступном в глобальной сети

Привязка к параметрам компьютера и активация. Механизм защиты прост, при установке программа генерирует ключ и при запуске считывает оборудование и опять генерирует ключ, проверяя соответствии с первоначальным ключом при каждом запуске. При смене конфигурации компьютера такой вид защиты приводит к неработоспособности ПО.

Защита кода от анализа. Отдельный вид защиты предполагает использования методов запутывания кода программы для противодействия копированию или модификации. Метод затрудняет, но не исключает возможности разобраться в коде, защищенном таким методом.

Защита с помощью простой аутентификации. Классическая защита доступа к приложению посредством ввода логина и пароля пользователя которые предоставляются пользователю по закрытым каналам связи при условии шифрованного хранения в самом приложении может достаточно хорошо защитить приложения от несанкционированного использования. Устойчивость данного метода защиты зависит от устойчивости логина и пароля к подбору, а также от безопасности каналов передачи. При соблюдении указанных данный метод может быть использован для реализации эффективной защиты.

Защита посредством сеансовых ключей. Метод используется совместно с защитой простой аутентификацией. После ввода логина и пароля пользователю необходимо ввести сеансовый ключ. Сеансовый ключ может находится на пластиковой карте или предоставляться пользователю посредством sms. Такой метод защиты традиционно используется в банковской сфере при совершении платёжных операций. Однако такой метод может использоваться и для других программных решений. Достаточно новый метод доставки сеансовых ключей заключается в обращении к сторонним сервисам, которые предоставляют сеансовые ключи меняя их через определённый интервал времени.

Защита с помощью биометрических систем. Биометрические системы аутентификации — системы аутентификации, использующие для удостоверения личности людей их биометрические данные.

Биометрическая аутентификация — процесс доказательства и проверки подлинности заявленного пользователем имени, через предъявление пользователем своего биометрического образа и путём преобразования этого образа в соответствии с заранее определённым протоколом аутентификации.

Не следует путать данные системы с системами биометрической идентификации, каковыми являются, к примеру системы распознавания, лиц водителей и биометрические средства учёта рабочего времени. Биометрические системы аутентификации работают в активном, а не пассивном режиме и почти всегда подразумевают авторизацию. Хотя данные системы не идентичны системам авторизации, они часто используются совместно. [2]

Для защиты доступа к приложениям можно использовать аутентификацию по лицу, голосу поскольку практически все современные ноутбуки и телефоны оснащены камерами и микрофонами высокого качества. К сожалению такую защиту можно взломать, зачастую не приложив никаких усилий. Многие системы распознавания ошибочно могут разрешить доступ по фотографии. Для обхода аутентификации по голосу можно использовать высококачественную запись. Несмотря на это биометрические системы осуществляют хороший уровень защиты совместно с другими методами защиты.

Эффективная защита. Основной принцип эффективной защиты современного программного обеспечения основан комбинировании методов защиты. Чем больше методов защиты используется, тем сложнее получить доступ. Однако использование большого количества методов защиты сказывается на удобстве пользователей и зачастую приходится искать компромисс между защитой и удобством.

Проблемы современных методов защиты. Из-за сильной зависимости от финансовой составляющей многие разработчики программного обеспечения не могут разработать собственную систему защиты и прибегают к сторонним разработкам что в свою очередь приводит к шаблонности систем защиты. Следствием такого является упрощения взлома.

В зависимости от сферы применения программного обеспечения. В игровой индустрии в последнее время чаще всего используется связка привязки аккаунта с ключом к компьютеру. Таким образом при изменении конфигурации компьютера пользователю нужно будет только подтвердить конфигурации временным ключом, присланным на email или телефон.

В сфере финансов чаще все распространена защита посредством электронных ключей совместно с проверкой компьютера пользователя по базе. Принцип работы прост в начале работы с программой пользователь авторизуется с помощью электронного ключа далее проверяется конфигурация его компьютера и сверяется с базой если компьютер не найден соединении блокируется.

В данной статье представлен обзор основных методов защиты от несанкционированного использования. Рассмотрены преимущества и недостатки также представлены комбинации методов, которые используются в современном программном обеспечении. На основании представленной информации в качестве системы защиты была выбрана комбинация серийного номера и привязки к параметрам компьютера.

ЛИТЕРАТУРА

1. Защита программного обеспечения [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Защита_программного_обеспечения. – Дата доступа: 23.09.2019.
2. Биометрические системы аутентификации [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Биометрические_системы_аутентификации. – Дата доступа: 23.09.2019.
3. Защита ПО от копирования и взлома: основные методы и стратегии [Электронный ресурс]. – Режим доступа: https://habr.com/ru/company/skillbox/blog/440836/. – Дата доступа: 23.09.2019.
4. Защита от несанкционированного копирования [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Защита_от_несанкционированного_копирования. – Дата доступа: 23.09.2019.