Защита и лицензирование

Программное обеспечение Guardant предоставляет эффективные инструменты для обеспечения защиты любого программного продукта. Guardant позволяет создавать системы защиты любого уровня сложности, в том числе, и такие, взлом которых будет невозможен или экономически невыгоден. Стойкость и надежность защиты напрямую зависит от степени продуманности и правильности установки системы защиты. Здесь описываются основные действия, которые необходимо выполнить для установки защиты. Системы защиты, основанные на использовании электронных ключей, могут выполнять ряд проверок различной степени сложности. Самые простые – проверки наличия ключа с заданными свойствами. Они выполняются быстро и могут использоваться достаточно часто. Более сложные проверки используют преобразование информации при помощи электронных ключей. Поскольку ключ является интеллектуальным устройством, он может выполнять преобразование информации по специальным алгоритмам. Разработчики системы защиты могут сами создавать дескрипторы алгоритмов и записывать их в память ключа при помощи утилит программирования. Такая возможность делает систему защиты уникальной.

ПО Guardant поддерживает два метода защиты:

- Автоматическая защита готовых приложений
- Защита при помощи Guardant API

Автоматическая защита

Метод основан на обработке готовых приложений утилитой автоматической защиты из состава ПО Guardant. В результате приложение привязывается к электронному ключу и получает защиту от отладчиков и дизассемблеров. Автозащита имеет множество режимов, которые позволяют настроить приложение на параметры электронного ключа (привязать его к ID, серийному номеру и т. д.), ограничить число запусков или время работы приложения и т. д.
Основное преимущество метода – в малом времени установки защиты. На сам процесс требуется всего несколько минут. Кроме того, для установки защиты не нужны специальные знания. Этот метод применим даже в тех случаях, когда отсутствует исходный код приложения, и нет возможности разработать систему защиты на базе Guardant API.
Главный недостаток метода в том, что он не может обеспечить приложению достаточной защищенности. Сама суть метода указывает на то, что защита не может составлять с приложением единого целого. Она устанавливается на уже готовое приложение, как бы «приклеивается» к нему, поэтому есть вероятность того, что она может быть снята хакером. Кроме того, метод не может обеспечить нестандартной логики работы защиты, что очень важно для повышения стойкости к взлому.
Схема работы автоматической защиты:

- Утилита автоматической защиты вписывает в тело защищаемого приложения исполняемый модуль – внутреннюю вакцину.
- В момент запуска приложения внутренняя вакцина вызывает из отдельного файла внешнюю вакцину.
- Внешняя вакцина производит необходимые проверки и преобразования и запускает защищенное приложение

Более подробную информацию см. в гл. Автоматические инструменты.

Защита при помощи Guardant API

Метод основан на использовании специальных функций Guardant API, собранных в объектных модулях. Функции API обеспечивают выполнение с ключом любых операций: поиска, чтения и записи памяти, установки аппаратных запретов, кодирования данных при помощи аппаратных алгоритмов и т. д. Для установки защиты по этому методу нужно вставить вызовы функций API в исходные тексты приложения и скомпилировать их с объектными модулями.
Главное преимущество метода в том, что он обеспечивает неизмеримо более высокий уровень защищенности. Защита (при правильной ее установке) образует с приложением неразрывное целое, следовательно, удалить ее хакеру весьма сложно.
Функции Guardant API позволяют выполнить с ключом любую операцию, обработать любой доступный участок его памяти – иными словами, возможности по конструированию защиты ограничены только фантазией и трудолюбием разработчика. Можно выстроить любую, даже самую нестандартную логику работы защиты, что значительно осложнит хакеру задачу ее взлома. Наконец, только функции Guardant API дают полную свободу действий по работе с аппаратными алгоритмами ключей.
Создание системы защиты, построенной на Guardant API – задача, допускающая множество различных решений. В силу этого невозможно дать универсальное и детальное, пошаговое описание процесса установки такой защиты. Ниже предлагается лишь общая схема действий, которой следует придерживаться в любом случае:

- Ознакомьтесь с функциями Guardant API при помощи **API Эксплорера** (файл **GAPIE_GUI_SE.exe**) и справки по Guardant API
- Изучите тестовые примеры программ на соответствующем языке программирования (см. каталог **"%ProgramFiles(x86)%\Guardant\SDK#\Samples"**). В тестах содержатся примеры использования функций Guardant API
- Разработайте свою систему защиты, используя приобретенные знания и рекомендации, содержащиеся в разделе **Защита при помощи API**

Какой метод выбрать?

Можно использовать эти методы по отдельности – только автоматическую защиту, либо только защиту с помощью API. Однако все сказанное выше заставляет сделать вывод о необходимости совместного использования обоих методов. Только так можно «сложить» достоинства методов и «вычесть», компенсировать их недостатки.

Используйте автоматическую защиту для того, чтобы защитить приложение от отладчиков и дизассемблеров, закодировать его тело, укрыть от посторонних глаз вызовы функций API. Кроме того – это прекрасный метод защиты от любопытства людей, не имеющих достаточных навыков взлома защиты.

Однако автоматическая защита должна быть лишь «внешним уровнем обороны». Ядро же ее должна составлять защита при помощи функций API. Именно ей нужно поручить всю основную работу: проверку ключа и реакцию на его отсутствие, работу с памятью и аппаратными алгоритмами и т. д. Особенно важно построить защиту таким образом, чтобы она стала неотъемлемой частью самого приложения, без которой оно просто перестало бы верно работать.