Псевдокод

Наиболее серьезная проблема при защите программного обеспечения – это противодействие различным средствам статического и динамического анализа кода. Цель разработчика защиты состоит в том, чтобы как можно более затруднить работу по реверсингу.
На сегодняшний день технология псевдокода, работающего на виртуальной машине, является наиболее актуальной и эффективной.
Суть технологии состоит в том, что определенные фрагменты исполняемых файлов дизассемблируются, анализируются и преобразуются в защищенный код некоторой уникальной защищенной виртуальной машины. Сама виртуальная машина генерируется тут же. Анализировать логику работы защищенного подобным образом кода существенно сложнее, чем стандартные инструкции Intel-совместимых процессоров, поскольку для него не существует никакого стандартного инструментария (отладчиков, дизассемблеров). Поэтому взломщику приходится все делать вручную, что занимает на несравнимо больше времени, чем использование готовых инструментов.
В каждой копии виртуальной машины уникальным образом реализуются:

- Набор внутренних команд псевдокода
- Множественный взаимный контроль целостности (для затруднения внесения изменений и установки точек останова)
- Обфускация кода виртуальной машины (замусоривание реального кода вторичным)
- Преобразование кода самой виртуальной машины
- Преобразование самого псевдокода
- Параметры многих команд рассчитываются только во время выполнения (защита от статического дизассемблирования)
- Отсутствие постоянных сигнатур в защищенном псевдокодом коде (чтобы затруднить поиск такого псевдокода в защищенном приложении)

При помощи технологии псевдокода защищен код драйверов и Guardant API.