Преподу: Основной кусок бака. Пока описал только про IDA – почему выбрал ее. В разработке. Читать и ругать только то, что до pause. Сырое пока, но ничего, завтра поправлю и добавлю.

NEW!!

Исходными данными проекта явилась прошивка некоего устаревшего устройства (на базе TMS32054). В связи с этим был разработан и предложен следующий цикл разработки программного обеспечения:

1) Дизассемблирование прошивки.
2) Тестирование и анализ полученного кода.
3) Написание кодека на языке Си.
4) Первичное тестирование.
5) Модернизация кодека.
6) Повторное тестирование кодека.
7) Анализ полученных результатов.

Дизассемблирование – это ключ к исходному коду любой программы, будь это компьютерный вирус или любой другой бинарный файл. Транслирование исходного файла на язык ассемблер позволяет увидеть и изучить алгоритмы работы программы. Актуальность технологии бесспорна, хотя и является узкопрофильной. Именно поэтому сред дизассемблирования немного. К наиболее известным средам можно отнести: Sourcer, Hiew и IDA Pro. Каждый из них доказал свое право на существования, однако использоваться будет только один - IDA Pro. Этот выбор обуславливается положительными и отрицательными сторонами всех трех дизассемблеров:

1) *Sourcer* – один из простейших дизассемблеров. Позволяет конвертировать исходный файл в ассемблерный код, однако, примерно в 30% случаях требуется вмешательство программиста для исправления ошибок дизассемблирования, что делает не возможным отладку большой программы. Так же отсутствуют базы данных и интерактивность интерфейса – это неимоверно сказывается на удобстве, скорости и качестве обратной разработки.
2) *Hiew* - редактор двоичных файлов, ориентированный на работу с кодом. Имеет встроенный дизассемблер для x86, x86-64 и ARM, ассемблер для x86, x86-64 [1]. Кроме того, данный редактор распространяется бесплатно. Однако в связи с тем, что Hiew разработан в начале 90-ых, интерфейс не удобен, что опять-таки только усложняет работу. А кол-во поддерживаемых форматов входных файлов и процессоров сильно ограничено.
3) IDA Pro (англ. Interactive DisAssembler) — интерактивный дизассемблер, отличается исключительной гибкостью, наличием встроенного командного языка. Поддерживает множество форматов исполняемых файлов для большого числа процессоров и операционных систем. Позволяет подключает отдельные модулей, направленные на работу с тем или иным процессором. Последние версии позволяет самостоятельно разрабатывать модули, например, под необходимый процессор, и встраивать их в IDA. На данный момент является лидером среди дизассемблеров на рынке. Позволяет в автоматическом и полуавтоматическом режиме проводить дизассемблирование. Несмотря на то, что среда разработана в 1992 года, среда позволяет изменять названия ф-ий и переменных, сохраняет искомую позицию, записывает изменения в базу данных (с возможным экспортом), позволяет выполнять переходы по адресам двойным кликом мыши. Существуют как платные, так и бесплатные версии среды, что позволяет ее использовать всем желающим.

Литература:

1) Краткое описание Hiew. URL: https://ru.wikipedia.org/wiki/Hiew

PAUSE