Использование MPU/PMP для защиты памяти в микроконтроллерных операционных систем реального времени

Байгудин Сергей Сергеевич
АО «Лаборатория Касперского»
125212, г. Москва, Ленинградское шоссе, д. 39А, стр. 2
Sergey.Baygudin@kaspersky.com

Введение

В целях разработки операционной системы реального времени (ОСРВ) для микроконтоллеров нами было проведено объёмное исследование представленных на рынке популярных микроконтроллерных ОСРВ. Это исследование в том числе включало в себя глубокий анализ рядя технических свойств как самих систем, так и модулей аппаратных платформ.

В данном докладе рассматриваются результаты этого исследования в части использования модулей защиты памяти в архитектурах ARM профиля M и RISC-V на примере их применения в наиболее функциональной на данный момент операционной системе реального времени Zephyr.

Привилегии потоков

Современные микроконтроллерные архитектуры предоставляют возможность исполнять аппаратный поток в привилегированном или непривилегированном режимах. В непривилегированном режиме игнорируется или запрещается исполнение определённых системных инструкций, ограничивается доступ к системным регистрам и регионам памяти определённых в модулях защиты. Базируясь на этом, в операционных системах реального времени реализуется три архитектурных подхода. В первом случае операционная система исполняет потоки исключительно в привилегированном режиме. Во втором случае ОСРВ исполняет потоки только в непривилегированном режиме. А при третьем подходе, как например в операционной системе Zephyr, потоки могут исполнятся как в привилегированном, так и непривилегированном режимах.

Модули защиты памяти

В микроконтроллерных архитектурах ARM модули защиты памяти называются Memory Protection Unit (MPU), а в RISC-V – Physical Memory Protection (PMP). Регистровые модели данных модулей значительно отличаются друг от друга, но функционально эти модули предоставляют одни и те же возможности – конфигурацию регионов памяти, к которым будет иметь доступ привилегированные или непривилегированные потоки исполнения. Выделяют три типа ограничений доступа к защищаемой памяти: нет доступа, доступ только на чтение и полный доступ на чтение и запись. Так же настраивается возможность исполнения программного кода из регионов памяти. Отдельно в архитектуре ARM реализуется системная карта памяти, которая может быть активирована в MPU как background регион.

Использование модулей защиты памяти

В зависимости от операционной системы реального времени и аппаратной архитектуры на которой она исполняется, применяются разные архитектурные решения по защите памяти, но общие подходы у них одинаковые. Так в операционной системе Zephyr по умолчанию ограничивается доступ к ПЗУ, хранящее коды исполняемой программы и константные данные, к ОЗУ, хранящее динамические данные, к стеку исполняемого потока, а так же производиться защита стек от его переполнения. Таким образом, в операционной системе Zephyr отводится четыре региона памяти для её системных нужд, а остальные регионы система использует для защиты локальных данных пользовательского непривилегированного потока. Каждый раз при смене контекста потока, планировщик перенастраивает в модуле защиты памяти пользовательские регионы и регионы стека. Такая перенастройка занимает определённое процессорное время.

Измерение времени перенастройки модулей защиты памяти

Использование модулей защиты памяти, также как и непривилегированных режимов исполнения потоков в ОСРВ безусловно требует дополнительных вычислительных ресурсов микроконтроллера.

Рассмотрев результаты измерений времени переключения потоков на примере операционной системы Zephyr, как по системному таймеру, так и при добровольной передаче процессора другому потоку, а также времени перенастройки модуля защиты памяти при смене контекста потоков на разных микрокотроллерных архитектурах, мы можем говорить о том, что безопасность при использовании модулей защиты памяти в операционных системах реального времени стоит тех дополнительных вычислительных ресурсов, что мы видим. При этом операционная система Zephyr может создавать потоки с разными привилегиями, что позволяет исполнять критические ко времени функции в привилегированном режиме, не теряя практически в производительности программно-аппаратного комплекса в целом.

Выводы

В результате исследования модулей защиты памяти в разных микроконтроллерных архитектурах и проведения измерений дополнительных вычислительных ресурсов при использовании MPU/PMP на примере операционной системы реального времени Zephyr, можно сделать выводы, что:

- использование MPU/PMP требует дополнительных вычислительных ресурсов для обеспечения безопасности;
- затраты на использование MPU/PMP составляют менее 0.5% от времени системного кванта (1 мс) при частоте микроконтроллера в 160 МГц;
- применение модулей защиты памяти приемлемо при разработке микроконтроллерных ОСРВ.

Ключевые слова

Операционная система реального времени, ОСРВ, Микроконтроллер, МК, Memory Protection Unit, MPU, Physical Memory Protection, PMP.