Аппаратные способы защиты информации для микроконтроллеров в архитектуре RISC-V.

Невидин Константин Вадимович, Синтакор. konstantin.nevidin@syntacore.com

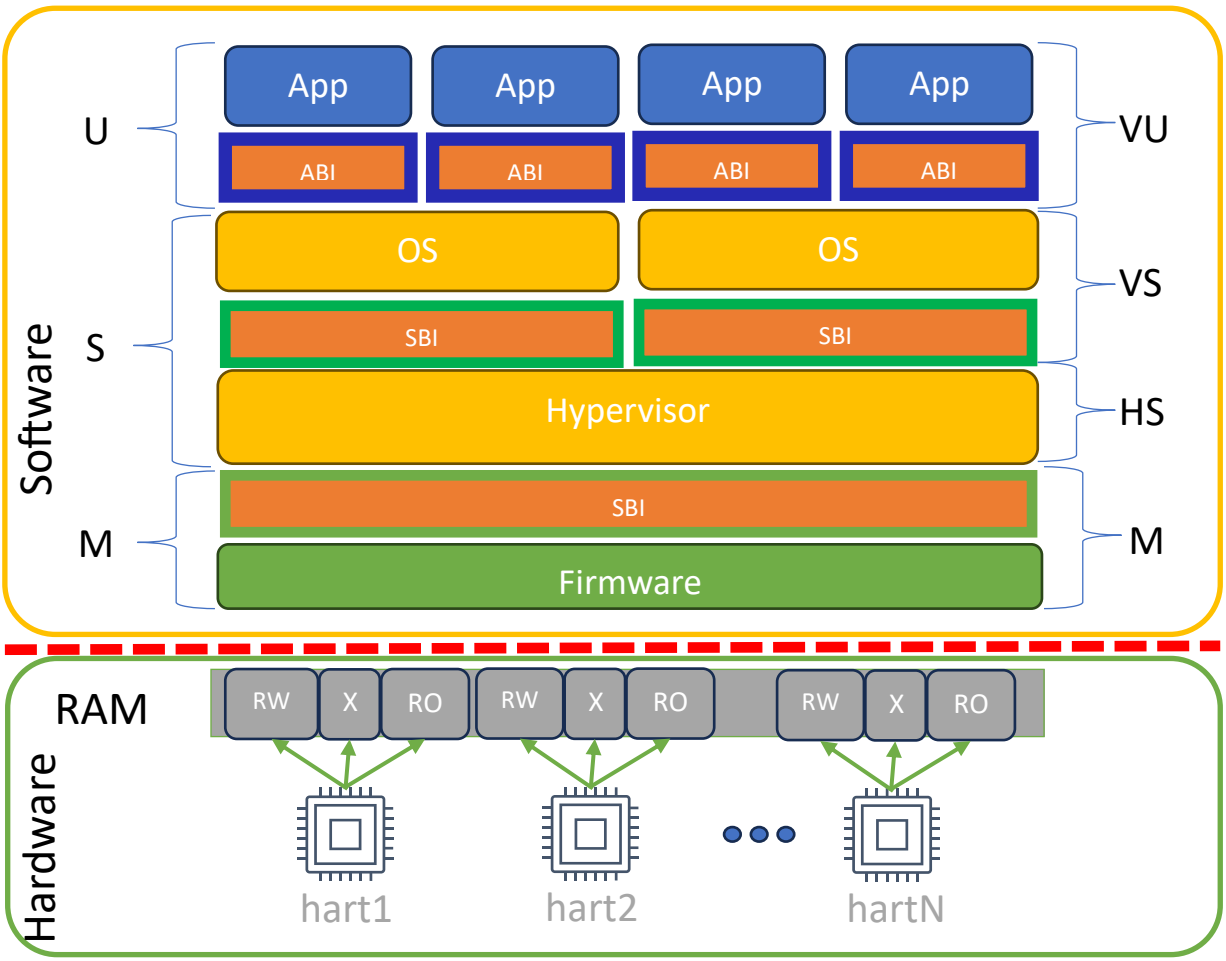
Микроконтроллеры в настоящее время являются неотъемлемой частью современной электроники и играют ключевую роль в автоматизации различных процессов. Эти миниатюрные компьютеры, объединяющие в себе процессор, память и периферийные устройства, находят широкое применение в промышленности, бытовой технике, медицинском оборудовании, автомобильной электронике и многих других сферах. Они обеспечивают управление сложными системами, обработку данных в реальном времени и взаимодействие с внешними устройствами. Благодаря компактным размерам, низкому энергопотреблению и высокой надёжности микроконтроллеры стали основой для создания умных устройств, от простых датчиков до сложных робототехнических комплексов. Их универсальность позволяет решать задачи различной сложности — от простого управления освещением до реализации сложных алгоритмов искусственного интеллекта, что делает их незаменимым компонентом современной технологической инфраструктуры.

Аппаратная защита информации в микроконтроллерах является критически важным аспектом современной электроники, поскольку эти устройства активно используются в системах, где безопасность данных имеет первостепенное значение. Микроконтроллеры, применяемые в умных устройствах, медицинских приборах, автомобильной электронике и промышленной автоматике, должны быть надежно защищены от несанкционированного доступа, взлома и модификации программного кода. Аппаратные механизмы защиты, такие как шифрование памяти, защита от чтения и записи, механизмы аутентификации и контроля доступа, обеспечивают фундаментальную основу безопасности, которая не может быть полностью заменена программными методами. Именно аппаратная защита гарантирует, что даже при физическом доступе к устройству злоумышленник не сможет получить доступ к конфиденциальным данным или изменить критически важные параметры работы системы.

Аппаратная защита информации в микроконтроллерах на базе архитектуры RISC-V реализуется через многоуровневую систему механизмов безопасности. Ключевым элементом является система привилегий, которая разделяет доступ к ресурсам процессора на несколько уровней:

- Machine (M)
- Machine (M), User (U)
- Machine (M), Supervisor (S), User (U)

Каждый уровень имеет свои права доступа к системным ресурсам и периферии.



В архитектуре продвинутых микроконтроллеров с поддержкой виртуальной памяти предусмотрены механизмы защиты памяти через систему MMU (Memory Management Unit), которая позволяет создавать изолированные области памяти с различными атрибутами доступа. Например, можно пометить определенные участки памяти как исполняемые только для чтения или доступные только для записи.

Важным элементом безопасности является Physical Memory Protection (PMP) для защиты от несанкционированного доступа к определенным областям памяти, выделенным каждому ядру/харту процессора. Для защиты памяти от несанкционированного доступа со стороны периферийных устройств используется расширение PMP для операций ввода-вывода IOPMP. Control Flow Integrity (CFI) механизм защиты, который обеспечивает целостность потока управления в программном обеспечении. Этот набор мер безопасности состоит из двух компонентов – теневой стек (shadow stack) и точки приземления (landing pads), предотвращающих несанкционированное изменение потока выполнения программы. Они служат для защиты от атак переполнения буфера, для предотвращения выполнения произвольного кода, для защиты от атак возврата в библиотеку (return-to-libc), для предотвращения спуфинга вызовов функций.

Практические примеры реализации защиты позволяю осуществить создание защищенных зон флеш-памяти для хранения криптографических ключей, изоляцию критических участков кода в отдельных областях памяти, внедрение механизмов безопасной загрузки (Secure Boot) и т.д.

Все эти механизмы работают совместно, создавая надежную основу для защиты микроконтроллеров от различных видов атак и несанкционированного доступа к данным.

В докладе будет представлен обзор методов аппаратной защиты процессоров уровня микроконтроллеров, реализованных и планируемых к реализации в экосистеме RISC-V.