Построение платформы безопасности перспективных вычислительных систем на архитектуре RISC-V для современных ОС

В динамично развивающемся цифровом мире любая современная ОС обладает широкими возможностями и обширным функционалом для удовлетворения запросов пользователей. Совместно с возможностями, кратно растет и число потенциальных уязвимостей в ОС, расширяя поверхность атаки со стороны потенциального злоумышленника, что ставит под угрозу пользователей и их персональные данные: «цифровые следы», пароли, ключи и другие активы. Закономерным следствием является стремление каждой ОС выстроить контур безопасности для защиты пользователя и его конфиденциальных данных балансируя между безопасностью и производительностью и опираясь на аппаратную платформу вычислительной системы.

Современные вычислительные системы имеют множество векторов развития, среди которых долгое время доминировала производительность. Однако в последние годы разработчики вычислительных систем поддерживая тенденцию на усиление безопасности программной среды, ищут компромисс между производительностью и безопасностью. Не стали исключением из этого «правила» вычислительные системы на достаточно молодой открытой архитектуре RISC-V, идущей по стопам своих именитых «товарищей». Сложная архитектура высокопроизводительных вычислительных систем с интегрированными аппаратными блоками безопасности затрудняет определение соответствия решения критериям необходимости и достаточности в построении безопасной аппаратной платформы. Архитектура RISC-V в своем развитии имеет хорошую возможность представить полный и непротиворечивый инструментарий для построения эффективной аппаратной платформы безопасности, учитывая накопленный опыт и ошибки решений на альтернативных архитектурах.

В докладе рассматриваются варианты построения аппаратных платформ безопасности перспективных вычислительных систем на архитектуре RISC-V, способных стать фундаментом для подсистем безопасности современных ОС или дополнить их.

Ключевые слова: Операционная система, Программная среда, Безопасность, Аппаратная платформа, RISC-V