ПОДХОДЫ К ПОСТРОЕНИЮ ДОВЕРЕННОЙ СРЕДЫ ИСПОЛНЕНИЯ В СОВРЕМЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ ПЛАТФОРМАХ

Габер П. Н., Диваков Н. В.
Группа Микропрограммного ПО, Отдел Системного ПО, ЗАО «Инженерный Центр ЯДРО»
Минск, Республика Беларусь
E-mail: p.gaber@yadro.com, n.divakov@yadro.com

Работа посвящена вопросу построения доверенной среды исполнения (ДСИ) для купирования угроз безопасности во встраиваемых системах, построенных на наиболее распространенных современных архитектурах. В ней рассматриваются варианты реализации ДСИ на программно-аппаратном уровне, а также приводится обзор существующих решений.

Введение

Современные средства вычислительной техники (СВТ) для работы прикладного программного обеспечения (ПО) предоставляют расширяемую универсальную среду исполнения (УСИ). УСИ обеспечивает гибкость взаимодействия и широкие функциональные возможности, однако оставляет устройство уязвимым для широкого спектра угроз безопасности, как компрометация, изменение или утрата данных. Решением, направленным на минимизацию ущерба от реализации угроз СВТ, является применение в их составе программно-аппаратного комплекса (ПАК) с доверенной средой исполнения (ДСИ) для изоляции данных, представляющих ценность, и для выполнения операций с такими данными.

В работе рассматриваются варианты реализации ДСИ на программно-аппаратном уровне, применяемые в вычислительных платформах (ВП) на основе современных микропроцессорных архитектур.

I. Угрозы безопасности ПАК

Угрозы безопасности ПАК по их цели можно разделить на угрозы, направленные на компрометацию чувствительной информации и угрозы, направленные на повреждение или уничтожение данных. По времени проведения атаки выделяют атаки времени исполнения и недокументированные возможности несанкционированного доступа (бэкдоры).

Атаки времени исполнения можно разделить на [1]:

1. Атаки на инструкции возврата/вызова (ROP/COP/JOP) используют уязвимости переполнения буфера для перезаписи инструкций возврата/вызова на стеке;
2. Атаки трансляции адреса для преодоления барьеров изоляции виртуальной памяти через подмену прав доступа используя уязвимости в модулях ядра УСИ;
3. Атаки нарушения безопасности памяти (Memory Safety Violations), например, использования памяти после освобождения, эксплуатируют известные ошибки в ПО;
4. Атаки по сторонним каналам используют анализ паттернов работы ЦПУ и непрямое воздействие на исполняемый код для поиска и извлечения данных из кэша.

II. Доверенная среда исполнения

ДСИ – это аппаратное или программно-аппаратное решение, реализующее среду исполнения, изолированную от УСИ, но имеющую канал для взаимодействия с УСИ.

ДСИ должна обеспечивать:

1. Безопасность активов, управляемых ДСИ;
2. Безопасное размещение и исполнение ДП, их изоляцию друг от друга;
3. Безопасное хранение конфиденциальных данных с обеспечением согласованности, целостности и привязки к ДСИ;
4. Защищенный коммуникационный канал связи между КП в УСИ и ДП в ДСИ, включая конечные точки в ДСИ;
5. Сервисы контроля целостности кода и данных УСИ и ее приложений.

В качестве безопасного контура ДСИ должна обеспечивать выполнение вычислений, критических для безопасного функционирования устройства и УСИ, а также конфиденциальность и целостность обрабатываемых данных.

ДСИ должна нейтрализовать следующие угрозы СВТ в случае компрометации УСИ:

1. Несанкционированный доступ и изменение критически важной информации, вмешательство в работу компонентов УСИ;
2. Запуск на исполнение недоверенных приложений;
3. Сокрытие попыток и фактов компрометации системы.

III. Варианты построения ДСИ на ВП

ДСИ может быть реализована различными способами в зависимости от архитектуры, области применения, и сложности СнК.

Вариант 1. ДСИ размещается на отдельной СнК со своими собственными аппаратными ресурсами (память, контроллеры ввода-вывода и т.п.) (см. рис. 1). Такой вариант реализации ДСИ

обеспечивает максимальный уровень изоляции компонентов ДСИ от УСИ и максимальный уровень безопасности.

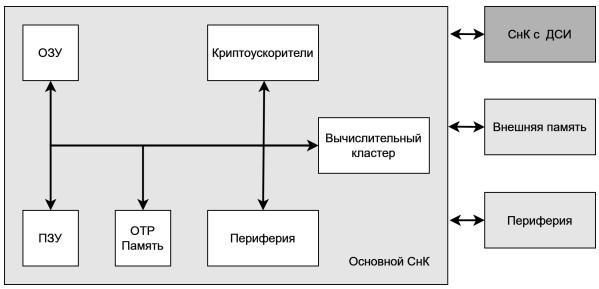

Рис. 1 – Размещение ДСИ на отдельной СнК

Вариант 2. ДСИ с использованием общих ресурсов с УСИ (см. рис. 2). Такой вариант предполагает что ДСИ выполняется на той же ВП, что и УСИ и совместно использует его аппаратные ресурсы. Разделение ДСИ и УСИ выполняется механизмами уровней безопасности (запуска), различными для ДСИ и приложений УСИ.

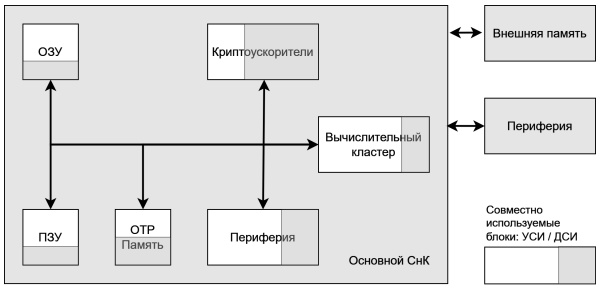

Рис. 2 – Совместное использование ДСИ и УСИ ресурсов СнК

Вариант 3. ДСИ с выделенным вычислительным ядром и аппаратными ресурсами (см. рис. 3). В этом случае для ДСИ выделяется одно из ядер СнК со своим набором ресурсов в изолированной подсистеме, которая имеет доступ к аппаратным ресурсам УСИ.

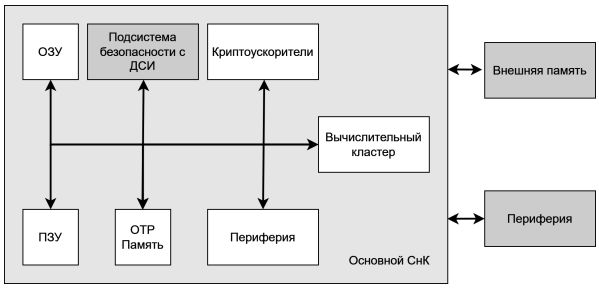

Рис. 3 – Выделенное ДСИ на общем СнК с УСИ

IV. Реализации ДСИ в современных архитектурах вычислительных средств

X86. В решениях компаний AMD и Intel используются различные подходы к реализации ДСИ. Intel Software Guard Extension (SGX) – это набор инструкций, который могут использоваться приложениями для создания защищенных областей кода и данных [2]. AMD Platform Security Processor (PSP) представляет собой сопроцессор на базе ARM (Cortex A5) с расширением TrustZone. Сопроцессор начинает работу до запуска основного вычислительного кластера и отвечает за верификацию UEFI загрузчика, его запуск и предоставление TPM сервисов [3].

ARM. Расширения безопасности ARM TrustZone позволяют разделять ресурсы и вычислительные ядра СнК на аппаратном уровне и создавать на их основе ДСИ. Изоляция КП и ДП выполняется с использованием защищенной памяти, контроллера прерываний, механизмами изоляции памяти и уровней безопасности (от EL0 до EL3) приложений [4].

RISC-V. На данный момент архитектура RISC-V не имеет стандартного механизма реализации ДСИ. На рынке присутствует несколько распространенных решений на базе RISC-V, которые базируются на расширении Physical Memory Protection (RISC-V PMP), которое использует специальные регистры для обеспечения механизма изоляции страниц памяти. SiFive WorldGuard решение является альтернативой ARM TrustZone. Оно использует специальные регистры для контроля прерываний, супервизор безопасности и три уровня исполнения кода для изоляции ДП от КП [5].

MIPS. MIPS TEE использует расширение виртуализации (VZ) и гипервизор L4Re для изоляции ДСИ (TEE) от УСИ (REE).

Заключение

В работе рассмотрены требования к реализации ДСИ, типовые варианты реализации и наиболее распространенные решения ДСИ на базе современных микропроцессорных архитектур.

1. Hardware-Enabled Security [Electronic Resource] / M. Bartock, M. Souppaya [and others]. – National Institute of Standards and Technology, 2022. – Mode of access: `https://nvlpubs.nist.gov/nistpubs/ir/2022/Nist.IR.8320.pdf`. – Date of access: 17.03.2023.
2. The Intel SGX Memory Encryption Engine [Electronic Resource] / S. Jonson. – Intel Software., 2016. – Mode of access: `https://software.intel.com/en-us/blogs/2016/02/26/memory-encryption-an-intel-sgx-underpinning-technology`. – Date of access: 17.10.2023.
3. AMD Platform Security Processor [Electronic Resource] / Wikipedia. – Mode of access: `https://en.wikipedia.org/wiki/AMD_Platform_Security_Processor`. – Date of access: 17.10.2023
4. Самоделов, А. Аппаратная поддержка доверенной среды исполнения в микроконтроллерах и микропроцессорах с архитектурой ARMv.8A и ARMv.8M / А. Самоделов // Материалы XXII научно-практической конференции «РусКрипто'2020». – 2020.
5. SiFive WorldGuard Technical Paper [Electronic Resource] / SiFive, 2023. – Mode of access: `https://sifive.cdn.prismic.io/sifive/f5dcaa9d-a0fd-4d91-b5e6-9ad4e5930c5e_WorldGuard-Technical-Paper_v2.4.pdf`. – Date of access: 17.10.2023.