ТЕХНОЛОГИЯ БЕЗОПАСНЫХ ВЫЧИСЛЕНИЙ

эльбрус

ТЕХНОЛОГИЯ БЕЗОПАСНЫХ ВЫЧИСЛЕНИЙ

Технология безопасных вычислений (ТБВ) — одна из ключевых возможностей, заложенных в архитектуру Эльбрус при проектировании, в соответствии с принципом secure by design. ТБВ — особый режим работы процессора Эльбрус, в котором аппаратура контролирует доступ в память не только к отдельным страницам, но и к отдельным объектам программы. ТБВ не допускает эксплуатацию злоумышленниками ряда уязвимостей, в том числе исключает «переполнение буфера». В процессе разработки ПО, при помощи ТБВ можно значительно ускорить процесс отладки, поскольку аппаратура процессора сама детектирует ряд ошибок и прерывает работу программы в момент возникновения ошибки (нарушения правил доступа к объектам в памяти), а не в момент проявления последствий этой ошибки.

В последнее десятилетие в мире резко возрос интерес к аппаратным средствам детального контроля над работой ПО. Среди наиболее значимых зарубежных проектов этого направления — британский проект CHERI, использование подобных технологий уже рекомендуется американскими регуляторами (Cybersecurity and Infrastructure Security Agency). Платформа Эльбрус с её промышленной реализацией ТБВ находится в этом тренде на лидирующих позициях.

SECURE BY DESIGN

ИСТОРИЯ ТБВ

В советских МВК Эльбрус-1, Эльбрус-2 и Эльбрус-3 ТБВ была реализована в полной мере, и основной объём системного и прикладного ПО работал под её управлением (рабочее название для ТБВ в то время – «защищённый режим исполнения»). Вся разработка программного обеспечения велась под управлением ТБВ, и его отладка происходила быстро и в комфортном для программистов режиме. Видимый результат — сдача в рекордно короткие сроки системы управления А-135 (ПРО Москвы), построенной на базе МВК Эльбрус-2. Эта система разрабатывалась разными коллективами по всей стране, содержала более 1 миллиона строк кода, и для программной разработки такой сложности наличие ТБВ стало решающим фактором успеха.

Эльбрус-2

А-135 «Дон-2Н»

ОСНОВНЫЕ КОМПОНЕНТЫ ТБВ

ИСПОЛЬЗОВАНИЕ ДЕСКРИПТОРОВ ВМЕСТО УКАЗАТЕЛЕЙ

В обычном режиме работы процессор Эльбрус, как и другие процессоры (x86, ARM, ...), использует для обращения к памяти *адреса* - числа, хранящиеся в 32- или 64-битных регистрах. Эти числа, с точки зрения процессора, не отличаются от любых других значений в памяти. В режиме ТБВ Эльбрус для обращения в память использует только *дескрипторы* — 128-битные структуры, которые хранят в себе: адрес обращения, базу объекта и размер объекта.

Для программиста на языке высокого уровня переход в режим ТБВ несложен. При переносе программы в режим ТБВ изменится размер указателя с 32 или 64 на 128 битов. Прочие операции с указателями в режиме ТБВ будут, как и в обычном режиме, проводиться согласно стандарту языка.

ОБЫЧНЫЙ РЕЖИМ

адрес

32 / 64 бита

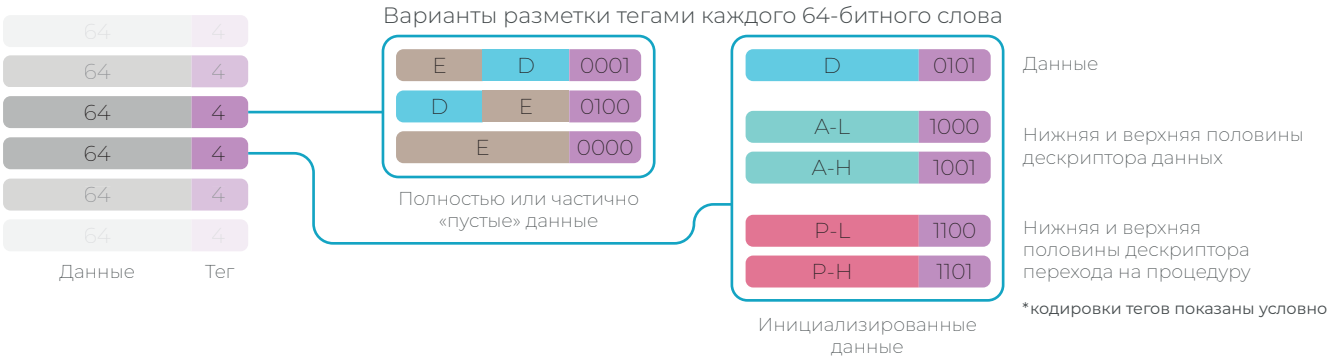
РЕЖИМ ТБВ

адрес	база	размер

128 битов

АППАРАТНОЕ ТЕГИРОВАНИЕ ПАМЯТИ

Для каждого выровненного 64-разрядного слова, процессор Эльбрус хранит в памяти 4-битный тег — «невидимое» значение, которое описывает тип данных, хранящихся в этом 64-разрядном слове. Типом может быть: пустое (неинициализированное) значение, данные, нижняя часть 128-битного дескриптора, верхняя часть 128-битного дескриптора (отдельно для работы с данными, отдельно для вызова процедуры). Как «пустые», могут быть отмечены отдельно верхние или нижние 32 бита данных. В других процессорах аппаратная поддержка тегов отсутствует, а программная — несёт очень высокие накладные расходы.



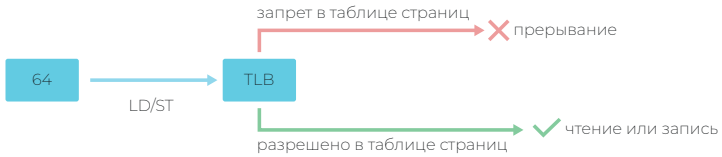
АППАРАТНЫЙ КОНТРОЛЬ ИНИЦИАЛИЗИРОВАННОСТИ ДАННЫХ

Если данные отмечены тегом «пустое значение», то процессор может их считать, но не может записать в память результат проведения над ними каких-либо операций. Если в ячейку памяти с тегом «пустое значение» записывается какое-либо число или дескриптор, то тег соответствующим образом корректируется.

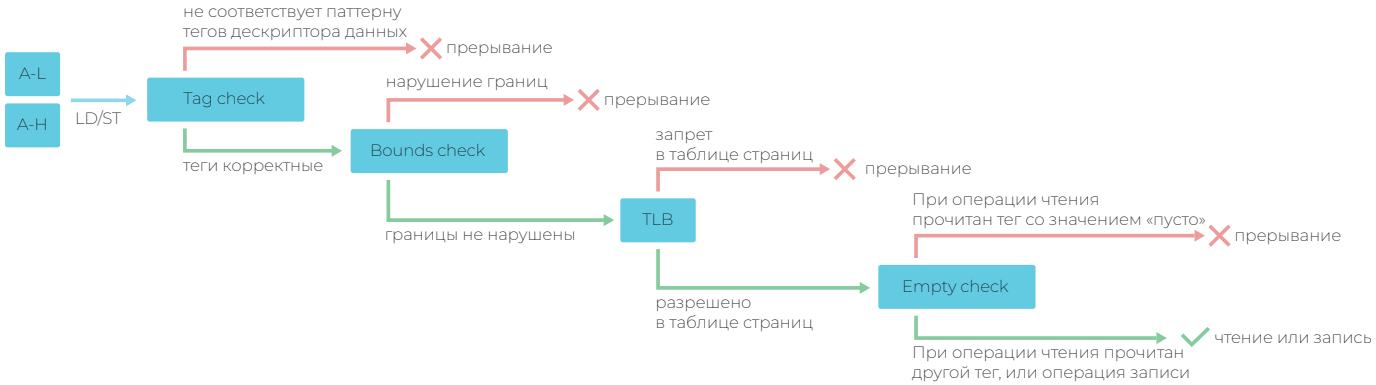
АППАРАТНЫЙ КОНТРОЛЬ ОБРАЩЕНИЙ ЧЕРЕЗ ДЕСКРИПТОРЫ

В обычном режиме работы процессора Эльбрус, как и у других процессоров (x86, ARM, ...), обращения в память контролируются только через таблицу страниц. В защищённом режиме, при обращении к памяти через дескриптор, процессор дополнительно проверяет, находится ли адрес обращения в границах, предписанных дескриптором. При нарушении границ вызывается прерывание. При вызове процедуры проверяется, что дескриптор предназначен для перехода, а не описывает область памяти с данными. Контроль границ происходит до передачи запроса в кэш-память, поэтому в режиме ТБВ исключается эксплуатация уязвимостей типа Spectre. За счёт системы тегов исключена возможность «напрямую» изменять части дескриптора, что гарантирует целостность системы контроля границ объектов.

ОБЫЧНЫЙ РЕЖИМ



РЕЖИМ ТБВ



ПОДДЕРЖКА В КОМПИЛЯТОРЕ, ЯДРЕ ОС И СИСТЕМНЫХ БИБЛИОТЕКАХ

На данный момент, ТБВ реализована для приложений в среде Linux (userspace). Для ТБВ адаптированы системные библиотеки и введена поддержка в ядре, а также реализован слой трансляции системных вызовов ядра. Это важная часть ТБВ, которая является дополнительным элементом проверки корректности данных, передаваемых в ядро при системном вызове.

ЗАДАЧИ, РЕШАЕМЫЕ ТБВ

- Обнаружение программных ошибок следующего типа:
  - Переполнение буфера
  - Использование неинициализированных данных
  - Обращение к уже освобождённому объекту в памяти (по зависшей ссылке)
- Защита от утечек по побочным каналам памяти типа Spectre.
- Предоставление разработчикам информационных систем новых способов разграничения доступа, более эффективных, чем имеющееся сегодня разделение адресных пространств процессов.

ОСОБЕННОСТИ ВНЕДРЕНИЯ ТБВ

Сегодня в режим ТБВ перенесён базовый набор системных библиотек. Основные проблемы, выявленные при портировании — использование аппаратно-зависимых приёмов программирования (явно и неявно сделанные предположения про размер указателей в битах, логические операции над указателями как над числами, преобразования указателей в числовые типы) и необходимость исправления найденных ошибок (в частности, инициализация всех данных и т.п.).

АО «МЦСТ» ведёт работу по дальнейшему переносу ПО в режим ТБВ, а также создаёт площадку для коллективной работы над этой задачей.

При всех своих полезных качествах, ТБВ незначительно уменьшает производительность (в среднем на 10–20 %) из-за дополнительных накладных расходов: увеличения потребностей в памяти, регистрах, затрат времени при инициализации вновь выделяемой памяти тегом «пусто» и т.п.

АНАЛОГИ ЗА РУБЕЖОМ

ТБВ интегрирована во все поколения микропроцессоров Эльбрус и долгое время в своём классе была единственной в мире. Сегодня наиболее близкий аналог — проект CHERI, который с 2010 года ведёт группа исследователей в Кембридже при содействии ведущих мировых производителей процессоров.

ЗНАЧЕНИЕ ТБВ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И УСТОЙЧИВОСТИ ИТ ИНФРАСТРУКТУРЫ РОССИИ

Безопасность информационных систем критически зависит от качества их программного кода. Порядка 70 % (согласно данным, приведённым в анонсе технологии ARM MTE) всех выявляемых уязвимостей сводится к ошибкам работы с памятью. Использование безопасных языков (Java, .NET и т. п.) не всегда возможно, и основной кодовой базой на обозримом горизонте остаётся экосистема Linux, ядро и основные системные компоненты в которой написаны на небезопасных языках Си и Си++. Многочисленные средства анализа и сертификации программного кода имеют ограниченную эффективность. Единственным средством надёжного обеспечения безопасности остаётся аппаратный контроль. Это отмечено в недавнем исследовании американского агентства по инфраструктурной безопасности, где предлагается использовать подход secure by design, а в качестве приоритетного примера – технология CHERI.

ТБВ — уже имеющаяся промышленная технология. Её продуктизация и широкое использование позволит в масштабах России значительно снизить риски информационной безопасности, улучшить качество российских продуктов, и повысить производительность труда программистов. Все эти эффекты отвечают на острые и актуальные проблемы, решение которых иными способами требует значительных усилий и средств.

ОНЛАЙН-ВЕРСИЯ ДОКУМЕНТА

АО «МЦСТ»: 117437, Москва, ул. Профсоюзная, д. 108
телефон: +7 (495) 363-96-65
факс: +7 (495) 363-95-99
e-mail: mcst@mcst.ru
Продажи: +7 (495) 797-81-91
sales@mcst.ru
Поддержка: +7 (495) 796-94-51
support@mcst.ru
Пресса: marketing@mcst.ru
Вакансии: resume@mcst.ru

www.mcst.ru