

Введение в современную архитектуру Intel

Горячий Максим Сергеевич

Сентябрь
2020

Описание курса

В курсе будут рассмотрены современные возможности архитектуры Intel.

Содержание курса

1. Обзор архитектуры IA-32/32e. Регистры и память. Регистры общего назначения, регистры x87/MMX/SSE/AVX/AVX-2/AVX-512, сегментные регистры, моделезависимые регистры (MSRs), модель памяти, адресное пространство ввода-вывода (I/O), configuration spaces.
2. Система команд. Команды общего назначения, команды математического сопроцессора, MMX, SSE, AVX, AVX-2, AVX-512. Команды передачи управления. Специализированные команды.
3. Режимы работы. Реальный режим (Real Mode). Защищённый режим (Protected Mode). Virtual-8086. System Management Mode. IA32e (Long Mode, режим совместимости).
4. Защищённый режим. Уровни привилегий. Сегментные дескрипторы. Сегментные регистры (CS, SS, DS, ES, FS, GS). GDT. LDT. Плоская модель памяти. Сегментация в Long Mode.
5. Кеш. UC/WC/WP/WT/WB типы памяти. MTRRs. PAT.
6. Paging. Структуры PDE, PTE. TLB. PAE. PDPE. IA-32e (PLM4E). Механизмы обеспечения безопасности: NX bit, SMAP, SMEP.

7. Обзор UEFI. Стадии загрузки. PEI и DXE драйверы. EDK2.
8. Поддержка многозадачности.
9. Передача управления. Call Gates. SYSCALL. SYSENTER. Автоматическое приключение стека. TSS. Task Gates.
10. Прерывания и исключения. Аппаратные и программные прерывания. Приоритет прерываний. APIC. Local APIC. Поддержка многопроцессорности.
11. Поддержка аппаратной виртуализации (Intel-VT_x). VMX Root Mode, Guest Mode. Virtual Machine Control Structure. VMLAUNCH, VMRESUME, VMEXIT. Shadow Page Tables. Extended (Nested) Page Tables. TLB Management with Virtualization.
12. *Обзор расширений для защиты данных. Intel SGX. Intel MPX.*
13. *Режим System Management Mode.*

Итоговые знания

- Базовое понимание архитектуры x86: регистры, память, режимы работы.
- Принципы работы виртуальной памяти в различных режимах работы процессора.
- Базовое понимание архитектуры UEFI, навыки разработки UEFI модулей.
- Что такое аппаратная визуализация и современные механизмы защиты.

Список литературы

- [1] Intel ® 64 and ia-32 architectures software developer's manual volume 1: Basic architecture.
- [2] Intel® 64 and ia-32 architectures software developer's manual combined volumes 2a, 2b, 2c, and 2d: Instruction set reference, a-z.

- [3] Intel® 64 and ia-32 architectures software developer's manual combined volumes 3a, 3b, 3c, and 3d: System programming guide.
- [4] Intel® 64 and ia-32 architectures software developer's manual volume 4: Model-specific registers.
- [5] Intel® 64 and ia-32 architectures optimization reference manual.
- [6] Agner Fog. Software optimization resources (assembly/c++).
- [7] Tom Shanley. *x86 Instruction Set Architecture*. MindShare Press.
- [8] Tom Shanley. *The Unabridged Pentium 4*. MindShare Press.
- [9] Гук М. *Процессоры Intel от 8086 до Pentium II*. Питер, 1998.
- [10] Гук М. *Процессоры Pentium III, Athlon и другие*. Питер, 2000.