Wintel Hell

A guide through nine circles of Dante’s technological inferno

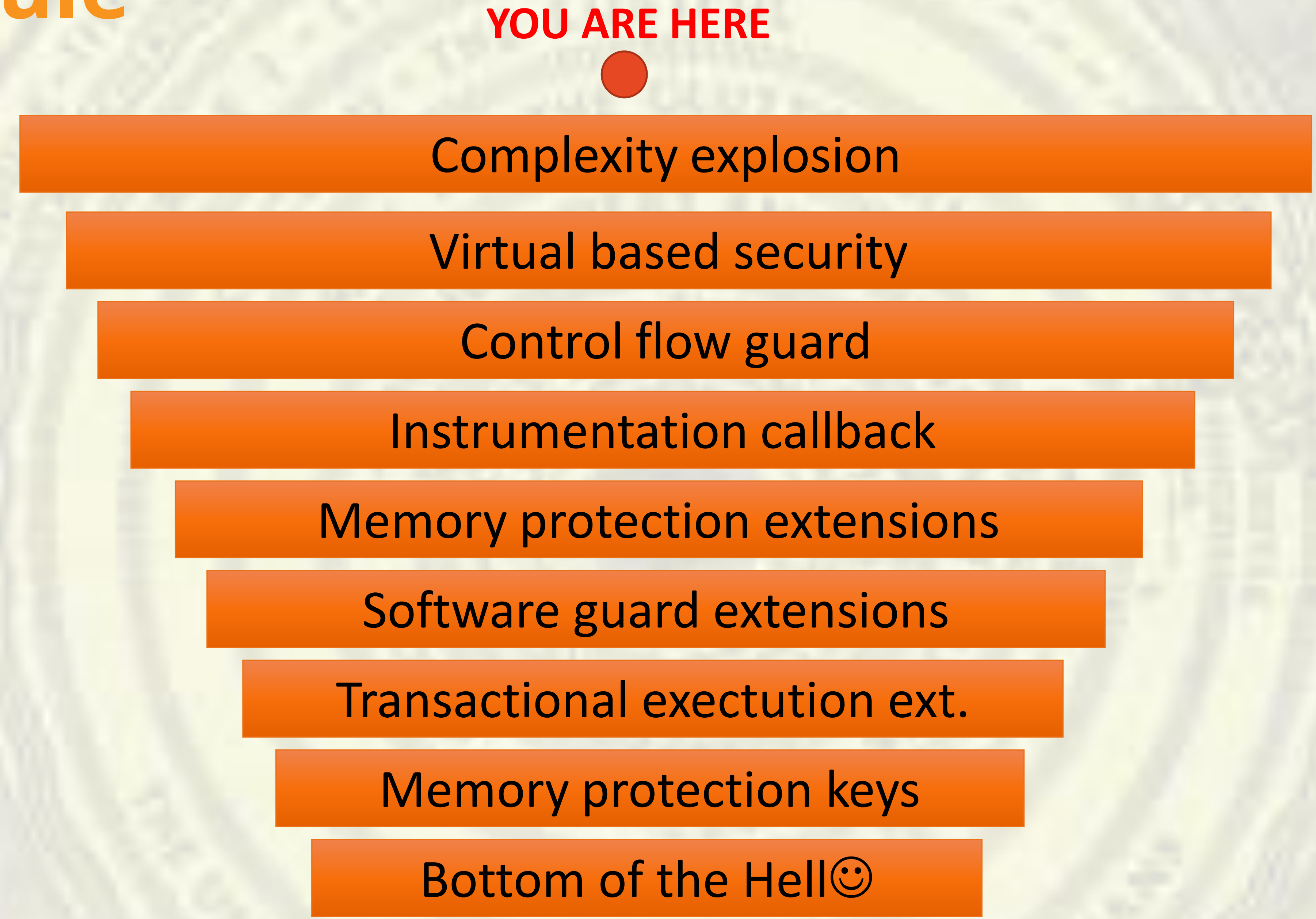
Martin Hron, researcher @ avast

SECURITY SESSION

CFG, VBS, VSM, SKM, MPX, TSX, SGX, MPK or PKU?

WHAT THE HELL?

Vestibule



YOU ARE HERE

Complexity explosion

Virtual based security

Control flow guard

Instrumentation callback

Memory protection extensions

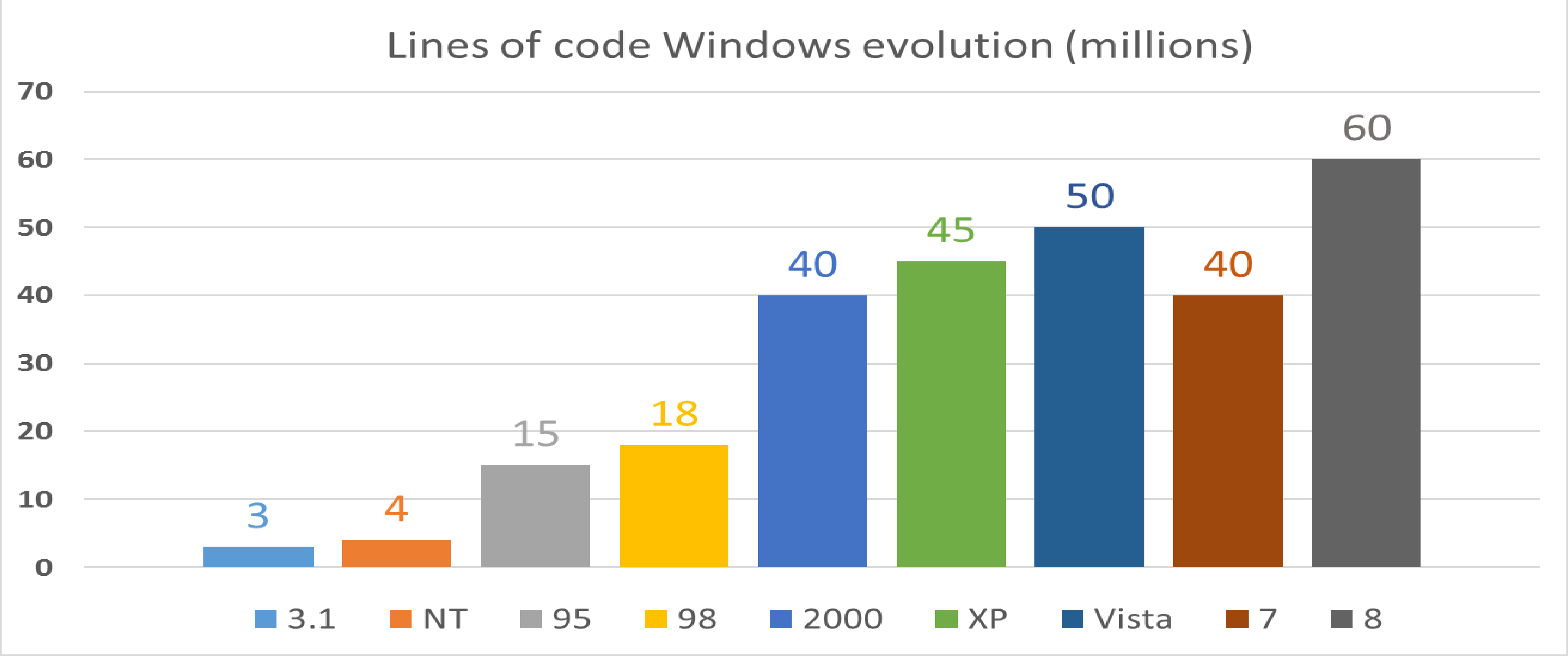
Software guard extensions

Transactional exectution ext.

Memory protection keys

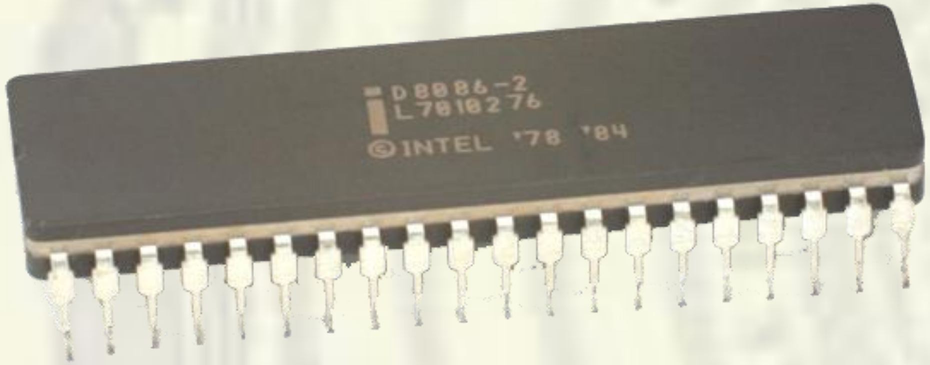
Bottom of the Hell☺

Circle 1 – Complexity explosion



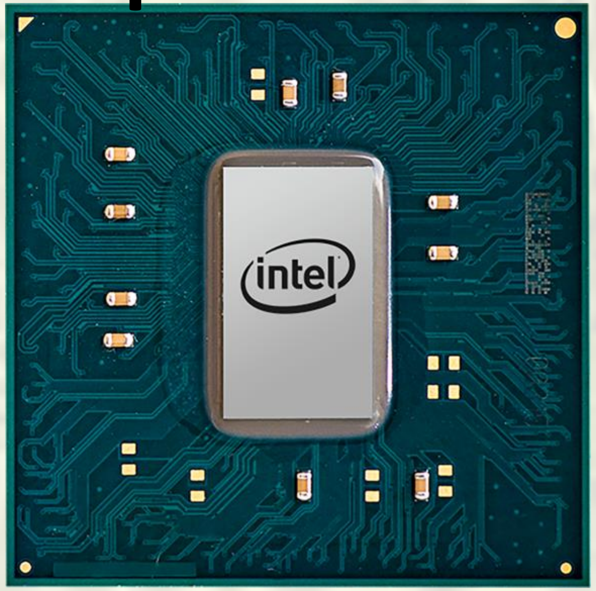
Circle 1 – Complexity explosion

Intel 8086



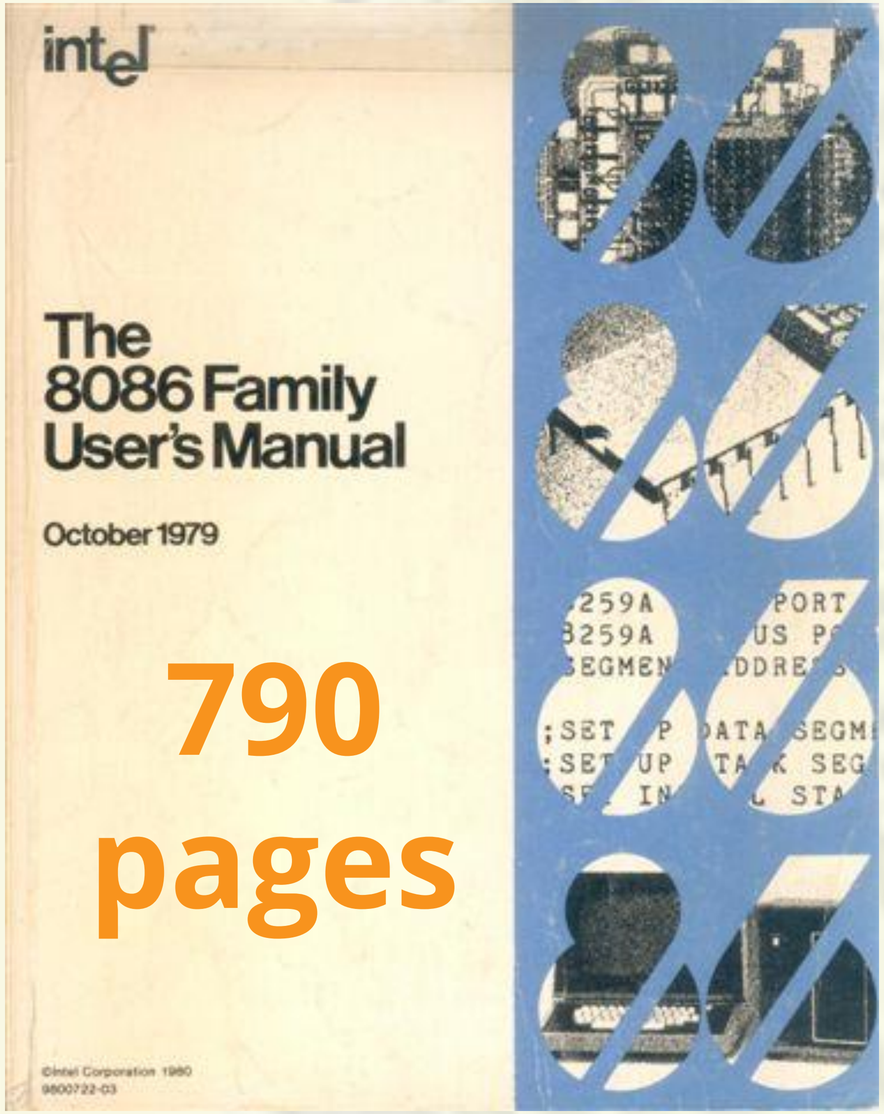
29,000 transistors
3,000 nm
33 mm^2 area

Intel 6th gen. SkyLake quad-core



1,750,000,000 transistors
14nm
122 mm^2 area

Circle 1 – Complexity explosion



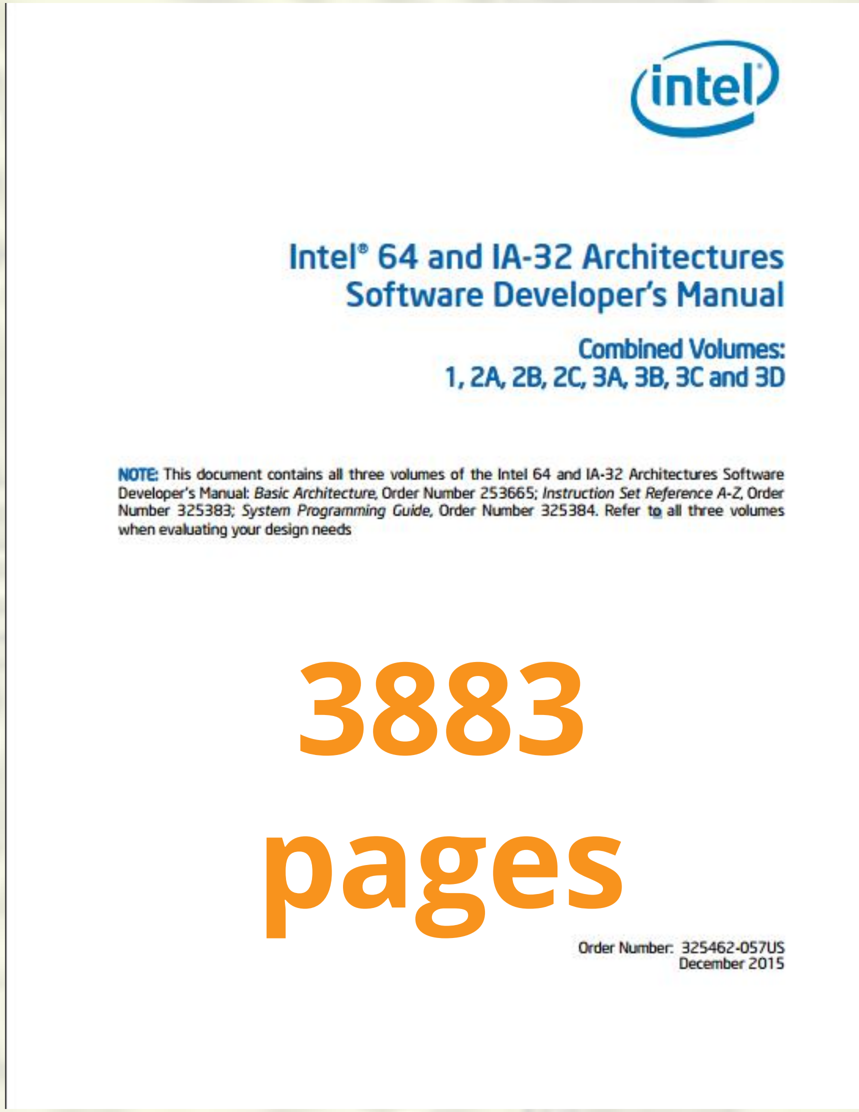
intel

The 8086 Family User's Manual

October 1979

©Intel Corporation 1980
9800722-03

790 pages



intel®

Intel® 64 and IA-32 Architectures Software Developer's Manual

Combined Volumes:
1, 2A, 2B, 2C, 3A, 3B, 3C and 3D

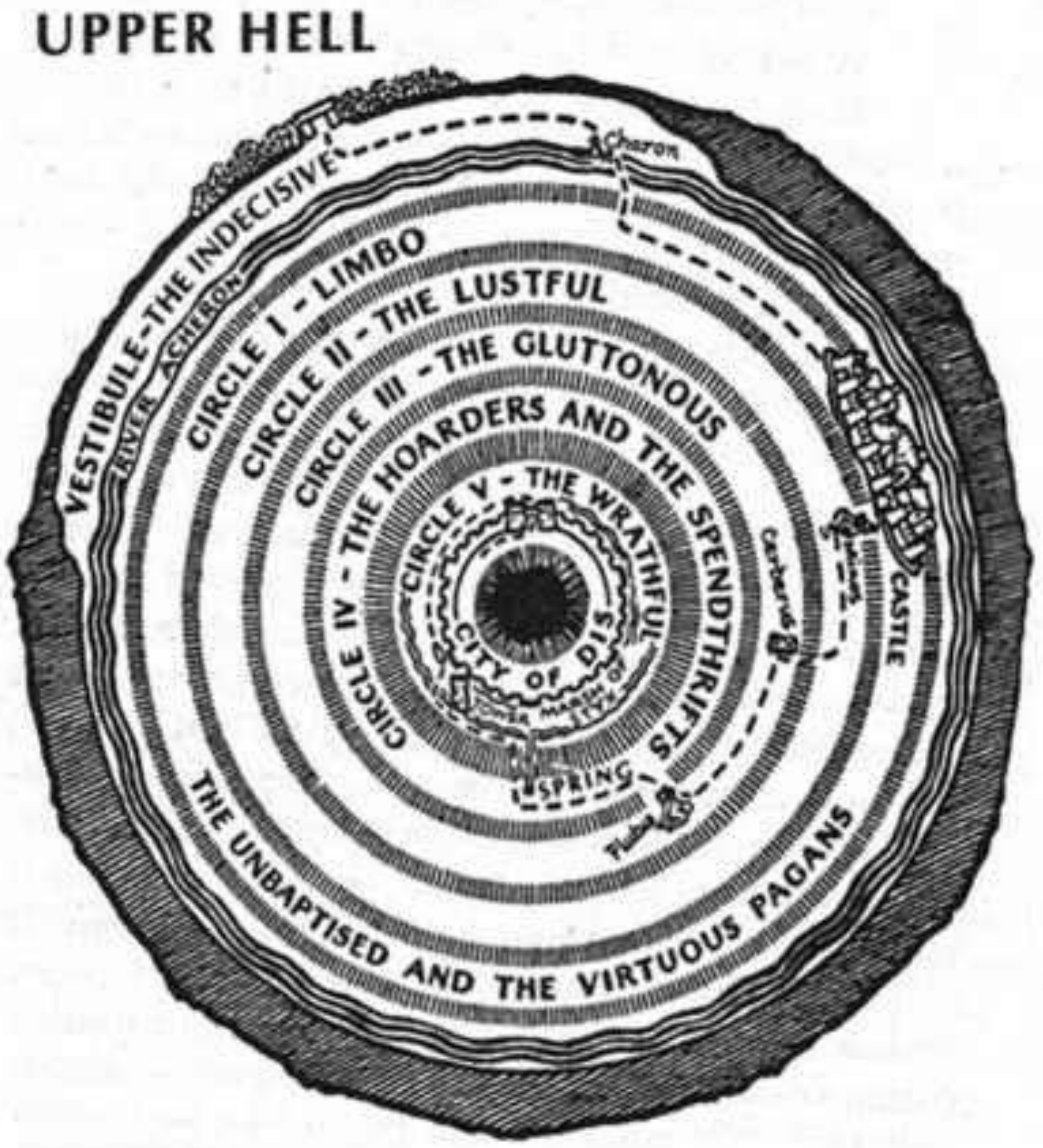
NOTE: This document contains all three volumes of the Intel 64 and IA-32 Architectures Software Developer's Manual: *Basic Architecture*, Order Number 253665; *Instruction Set Reference A-Z*, Order Number 325383; *System Programming Guide*, Order Number 325384. Refer to all three volumes when evaluating your design needs

Order Number: 325462-057US
December 2015

3883 pages

Upper Hell

Windows



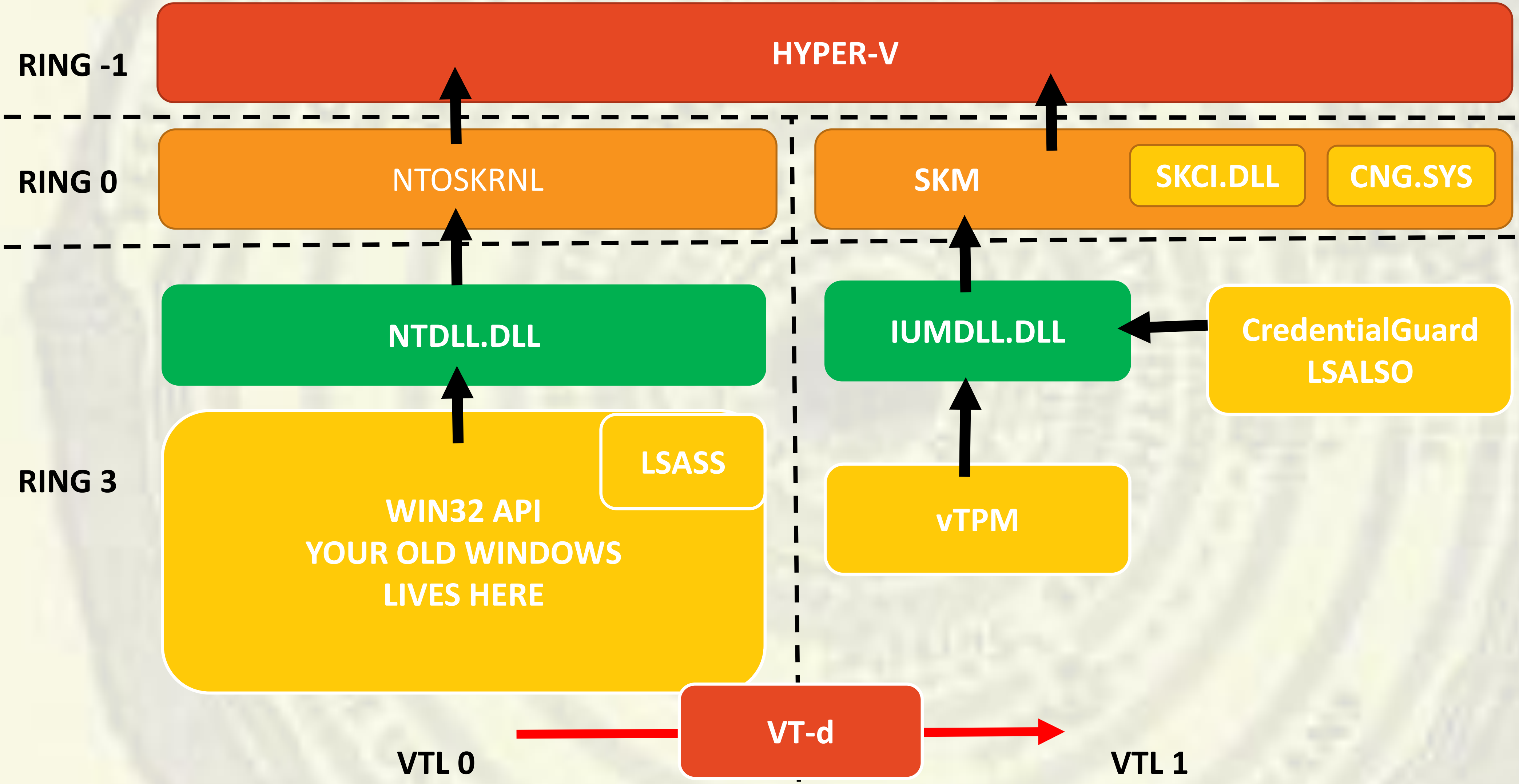
Circle 2 - VBS

virtual based security

- Windows 10 Enterprise and Server 2016
- Based on Hyper-V
- VSM Virtual Secure Mode
- Device Guard
- Credential guard
- Virtual TPM

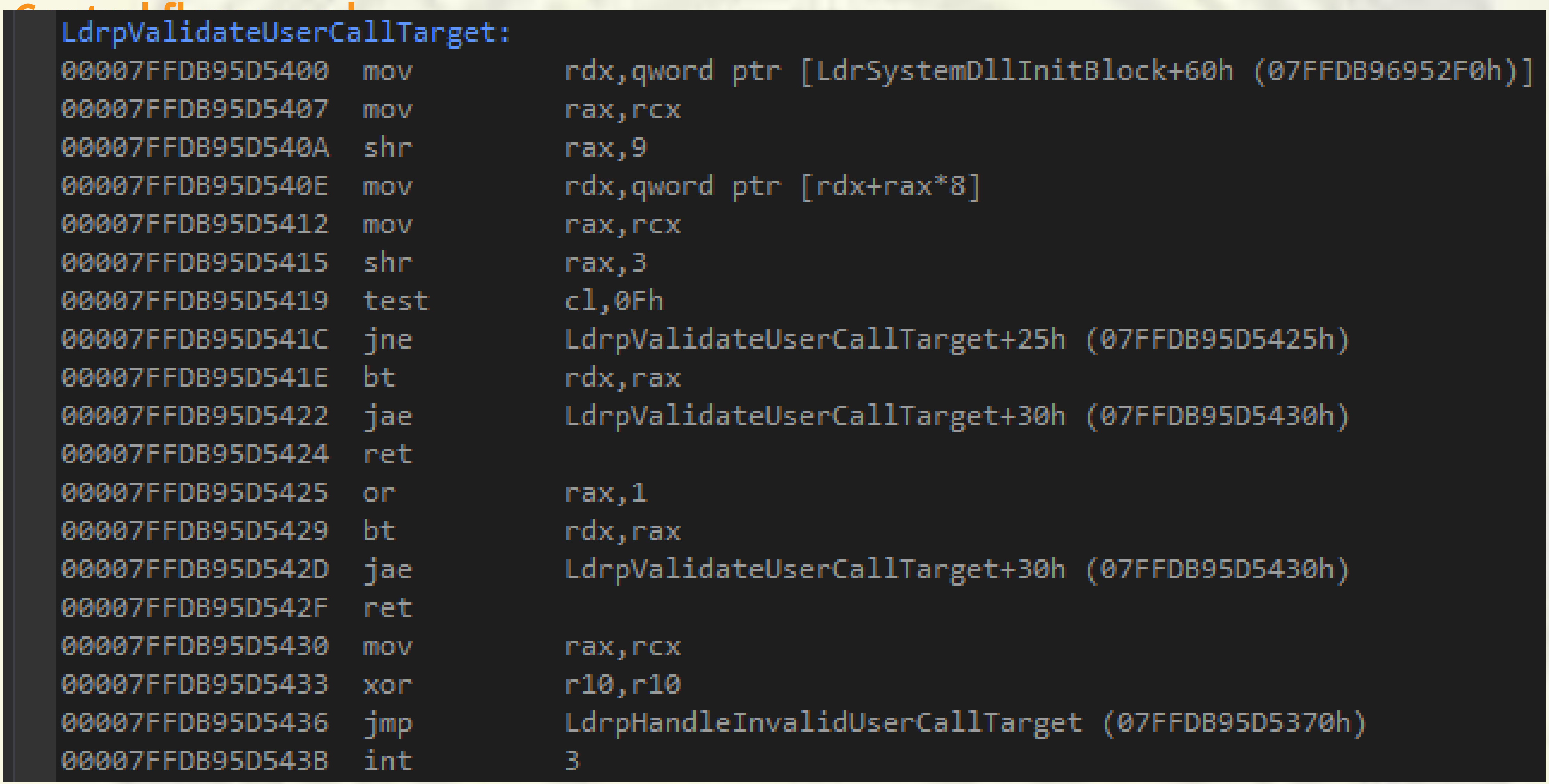
Circle 2 - VBS

virtual secure mode (VSM)



Circle 3 –CFG

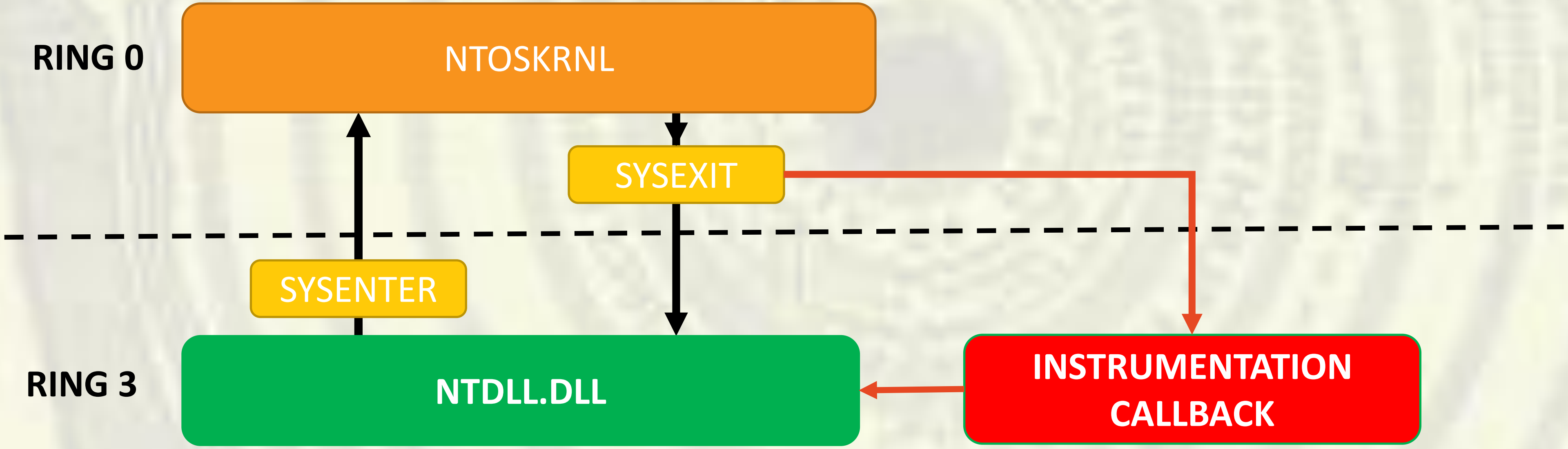
Control flow guard



```
LdrpValidateUserCallTarget:
00007FFDB95D5400  mov         rdx,qword ptr [LdrSystemDllInitBlock+60h (07FFDB96952F0h)]
00007FFDB95D5407  mov         rax,rcx
00007FFDB95D540A  shr         rax,9
00007FFDB95D540E  mov         rdx,qword ptr [rdx+rax*8]
00007FFDB95D5412  mov         rax,rcx
00007FFDB95D5415  shr         rax,3
00007FFDB95D5419  test        cl,0Fh
00007FFDB95D541C  jne         LdrpValidateUserCallTarget+25h (07FFDB95D5425h)
00007FFDB95D541E  bt          rdx,rax
00007FFDB95D5422  jae         LdrpValidateUserCallTarget+30h (07FFDB95D5430h)
00007FFDB95D5424  ret
00007FFDB95D5425  or          rax,1
00007FFDB95D5429  bt          rdx,rax
00007FFDB95D542D  jae         LdrpValidateUserCallTarget+30h (07FFDB95D5430h)
00007FFDB95D542F  ret
00007FFDB95D5430  mov         rax,rcx
00007FFDB95D5433  xor         r10,r10
00007FFDB95D5436  jmp         LdrpHandleInvalidUserCallTarget (07FFDB95D5370h)
00007FFDB95D543B  int         3
```

Circle 4 - Instrumentation Callback

- present in WIN7 since version 7 (probably), WIN10 changed few things
- can be set by just one call to **NtSetInformationProcess**



Lower Hell

CPU

Circle 5 – MPX

Memory Protection Extensions

- Supported on SkyLake, VS2015 Update 1 (/d2MPX), special Intel driver needed on Windows
- allows to check if pointer is inside bounds
- low overhead, can be turn on/off on demand
- equivalent to NOPS if disabled
- 4 BNDx 128 bit registers, storing upper and lower bounds for checked pointer
- Check instructions BNDCL, BNDCU
- BNDSTX and BNDLDX instruction associates range with pointer and store them into special table

Circle 6 – TSX

Transactional Synchronization Extensions

- First introduced on Haswell (4th generation)
- Comes in two flavours:
  - RTM Restricted Transactional Memory
  - HLE Hardware Lock Elision
- Works like real transaction
- EAX register contains reason of abort
- XBEGIN, XEND, XABORT, XTEST instructions

```
RETRY:
        or eax, 0FFFFFFFFh
        xbegin L0
L0:
        cmp eax, 0FFFFFFFFh
        jne L1
        inc qword ptr [rbp]
        xend
        jmp L2
L1:
        jmp RETRY
L2:
```

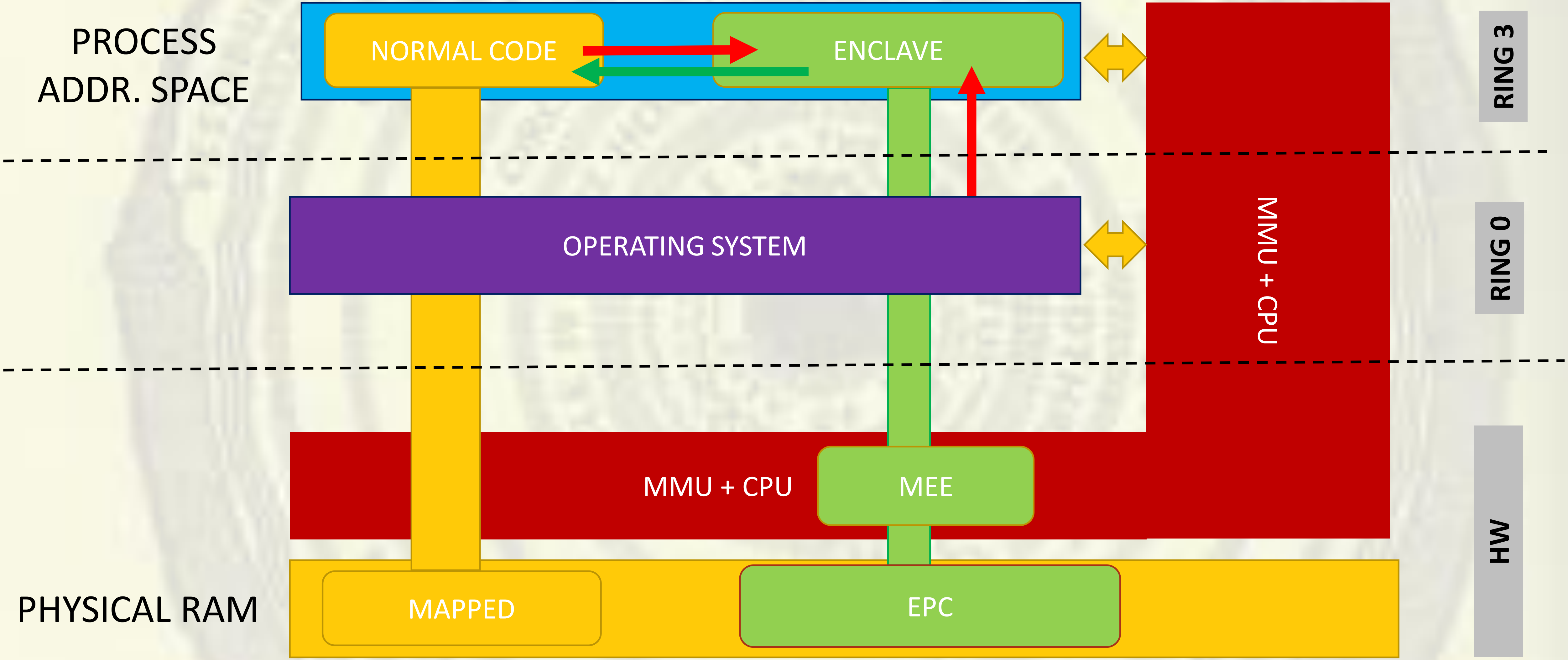
Circle 7 – SGX

Software Guard Extensions

- Supported on later SkyLake CPUs, WIN 10 Fall Update (October 26th)
- Allows creating protected part of application which is isolated
- Enclave could be only run through well known entry point
- No privilege level or even HW has access when it runs
- Content is always encrypted in physical RAM

Circle 7 – SGX

Software Guard Extensions



Circle 8 – MPK

Memory protection keys

- In upcoming processors “Kaby Lake” or “CannonLake”
- You can divide address space to 16 regions and change access by just flipping value in one register **PKRU**
- For certain applications this is huge speedup, because you don’t need to flush **TLB** cache.

The protection-key feature provides an additional mechanism by which IA-32e paging controls access to usermode addresses. When CR4.PKE = 1, every linear address is associated with the 4-bit **protection key** located in bits **62:59** of the paging-structure entry that mapped the page containing the linear address (see Section 4.5). The **PKRU** register determines, for each protection key, whether user-mode addresses with that protection key may be read or written.

Microsoft

Circle 9: deep at the bottom of the Hell

Known bugs notes and conclusion

- SkyLake CPUs are freezing at microcode level when running Prime95 test with special exponent. **Fixed by microcode update in 01/2016**
- Haswell and first Broadwells TSX: In August 2014 **bug has been identified** and this **feature was disabled by microcode update**
- SGX is not present in all SkyLake processors
- current errata contains, approx. 100 known bugs
- don’t trust your CPU, always detect features using CPUID and/or it’s side effects.

Control Flow Guard demo

Tools used

SAMSUNG
LAPHROAIG
ISLAY SINGLE MALT
SCOTCH WHISKY
SELECT
1815

Go ahead and ask!

And I’ll try to answer.

github repos with detailed documentation:

https://github.com/thinkcz/SecuritySession2016

I’ll be around till the end of conference.
Find me or send me PM via twitter if you want to ask: **@thinkcz**

GITHUB REPO

Thank you!

avast!

Microsoft

intel

no starch press
the finest in geek entertainment

LAPHROAIG
SINGLE ISLAY MALT
SCOTCH WHISKY

Martin Hron

E: martin@hron.eu

T: @thinkcz