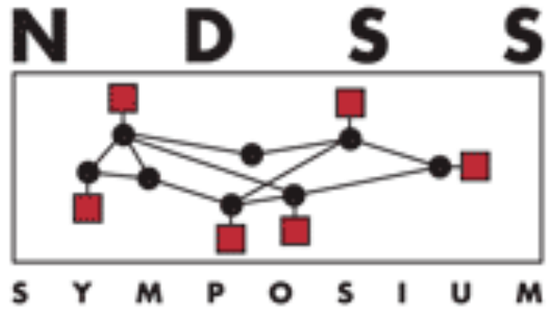
Practical Timing Side Channel Attacks Against Kernel Space ASLR

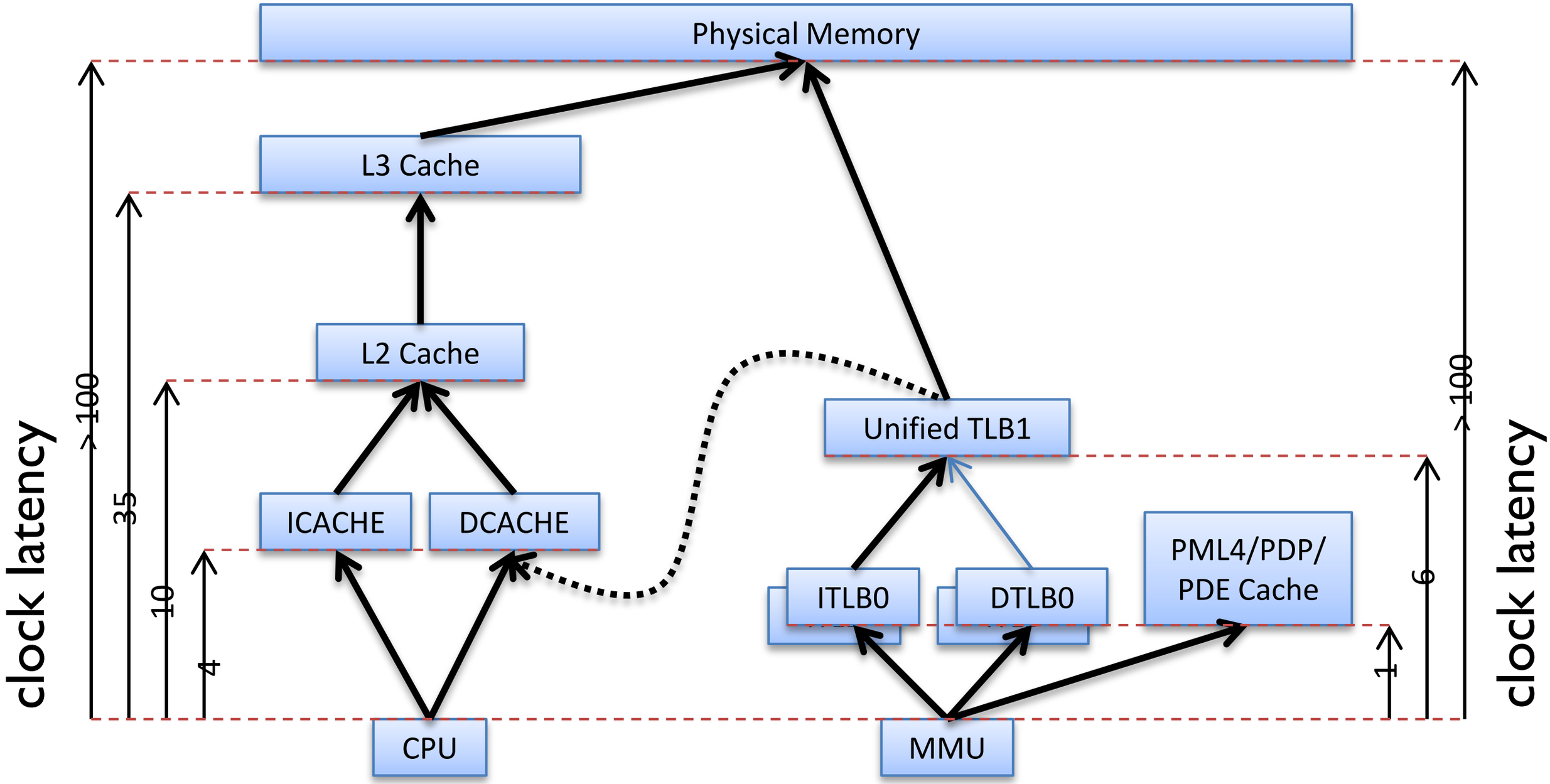
Ralf Hund, Carsten Willems and Thorsten Holz
Ruhr-University Bochum



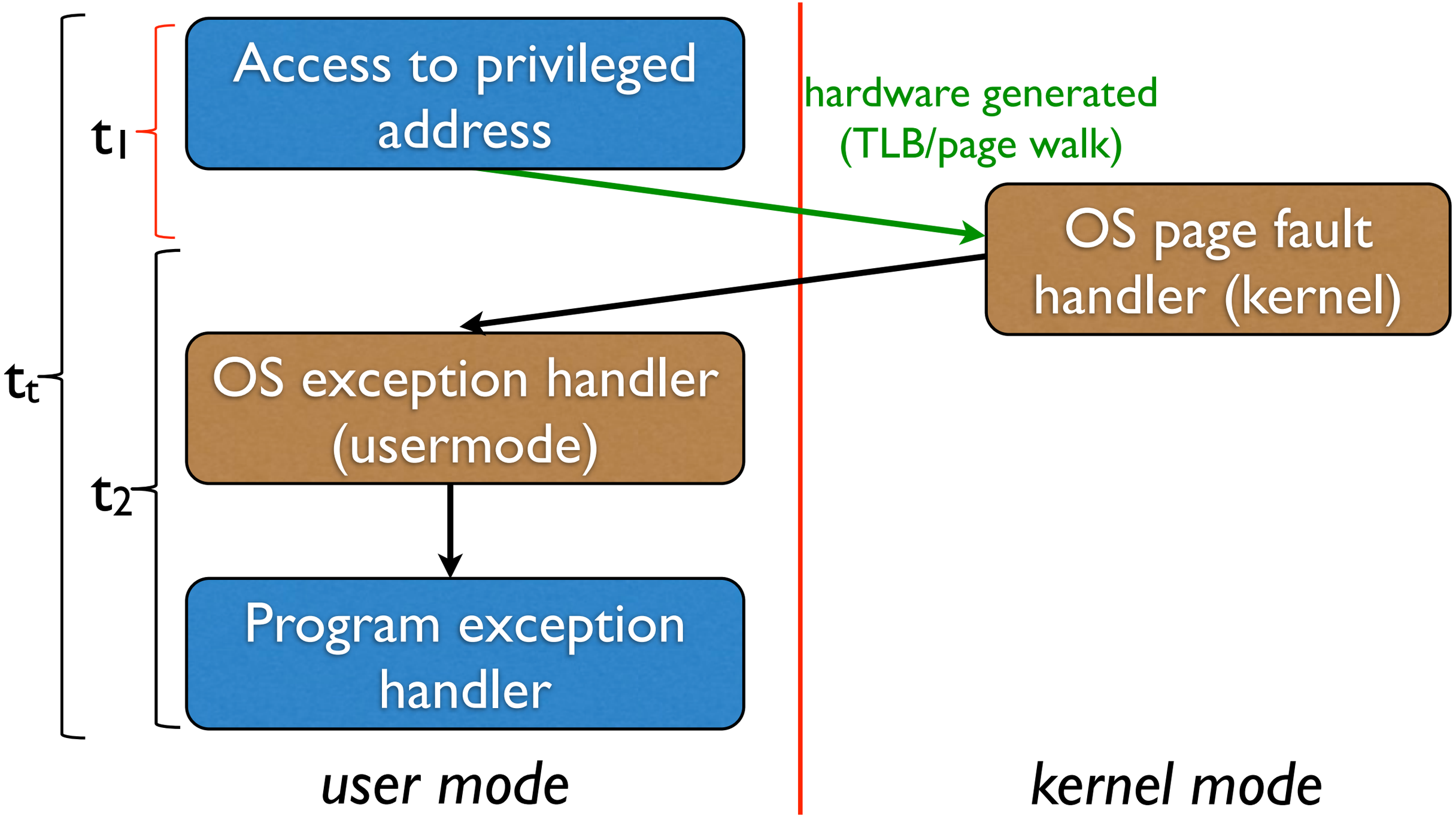
Motivation

- Combination of DEP and ASLR prevents many attacks
- Attacker model
  - Adversary has only restricted access (i.e., user mode)
  - Presence of a user mode-exploitable vulnerability within kernel or driver code (common problem)
  - Full user + kernel ASLR, DEP, no info leaks
- Goal: *de-randomize kernel space ASLR*

Memory Hierarchy



Memory Hierarchy



Approach

- Hardware is shared between privileged and non-privileged code ➠ side-channel attacks possible

  1. Set the system in a specific state from user mode
  2. Measure duration of a certain memory access
  3. Timing (possibly) reveals info about memory layout

- Attacks on L1/L2/L3 caches and TLB/PS caches
  - Cache probing, double page fault, cache preloading
  - Details in the paper (*published at IEEE S&P'13*)

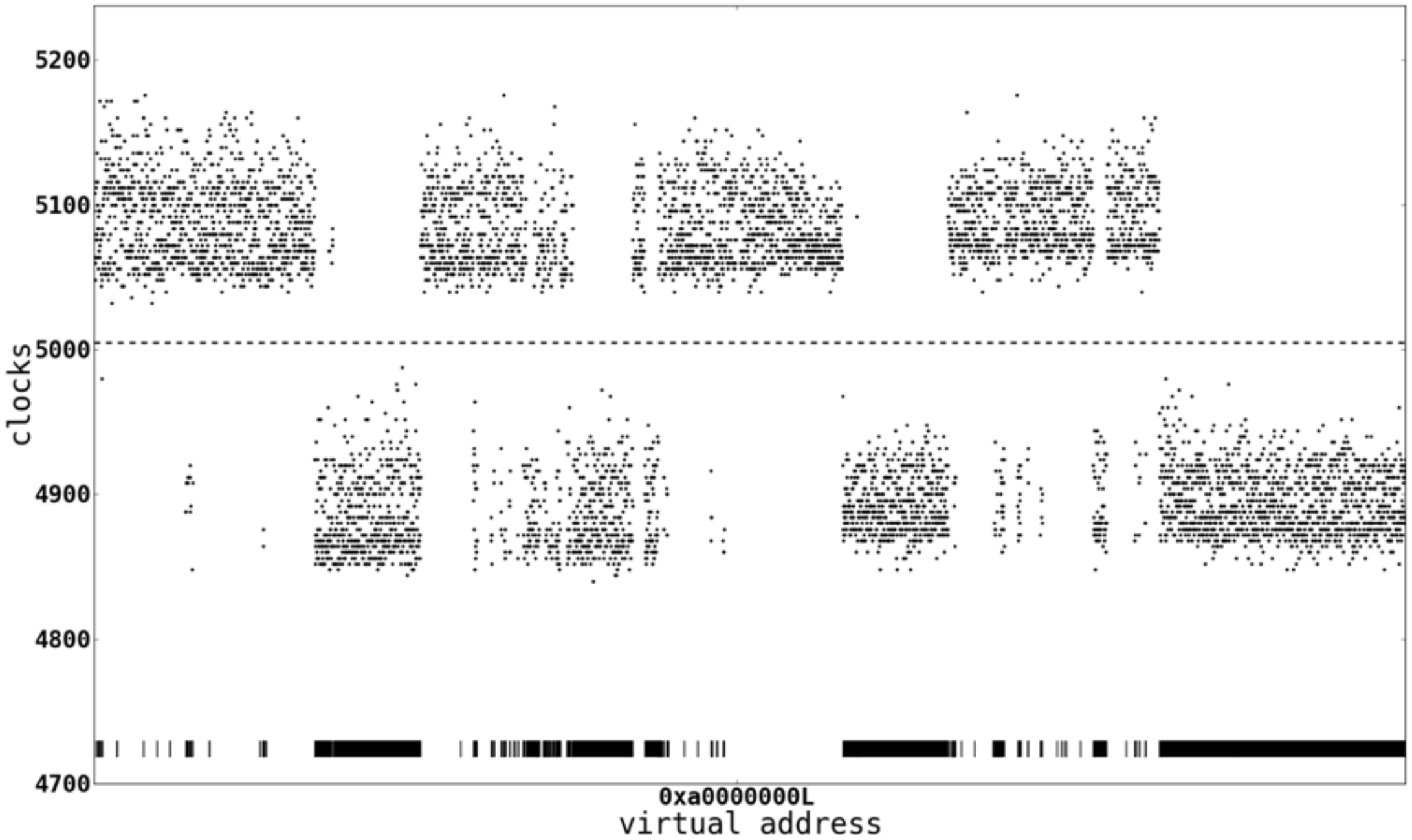
Results

- Tested on 32-/64-bit systems running Windows 7/Linux
- Tested on different CPUs + VM:
  - Intel i7-870 (Nehalem/Bloomfield, Quad-Core)
  - Intel i7-950 (Nehalem/Lynnfield, Quad-Core)
  - Intel i7-2600 (Sandybridge, Quad-Core)
  - AMD Athlon II X3 455 (Triple-Core)
  - VMWare Player 4.0.2 on Intel i7-870 (with VT-x)

Results

Method	Requirements	Results	Env
Cache probing	large pages or PA of eviction buffer	`ntoskrnl.exe` and `hal.sys`	all
Double page fault	none	allocation map, several driver	all but AMD
Cache preloading	none	location of `win32k.sys`	all

Results


5200
5100
5000
4900
4800
4700
clocks
0xa0000000L
virtual address

Questions?

Contact:
Thorsten Holz
thorsten.holz@rub.de

More info
http://syssec.rub.de