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

Physical Memory

L3 Cache

L2 Cache

ICACHE
DCACHE

CPU

Unified TLB1

ITLB0
DTLBO

PML4/PDP/PDE Cache

MMU

clock latency

clock latency
Memory Hierarchy

Access to privileged address

Hardware generated (TLB/page walk)

OS page fault handler (kernel)

OS exception handler (usermode)

Program exception handler

User mode

Kernel mode
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

<table>
<thead>
<tr>
<th>Method</th>
<th>Requirements</th>
<th>Results</th>
<th>Env</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cache probing</td>
<td>large pages or PA of eviction buffer</td>
<td>ntoskrnl.exe and hal.sys</td>
<td>all</td>
</tr>
<tr>
<td>Double page fault</td>
<td>none</td>
<td>allocation map, several driver</td>
<td>all but AMD</td>
</tr>
<tr>
<td>Cache preloading</td>
<td>none</td>
<td>location of win32k.sys</td>
<td>all</td>
</tr>
</tbody>
</table>
Results

Systems Security
Ruhr-University Bochum

Practical Timing Side Channel Attacks Against Kernel Space ASLR
Questions?

Contact:
Thorsten Holz
thorsten.holz@rub.de

More info
http://syssec.rub.de