



openHPI – Internet Security Excursion: Meltdown & Spectre

Prof. Dr. Christoph Meinel
Hasso Plattner Institute, Potsdam, Germany

Meltdown & Spectre – Worst Computer Vulnerabilities Ever

January 3, 2018: Security researchers publish two attacks – „Meltdown“ and „Spectre“ – that affect modern microprocessors

- Attacks work independently from operating systems, they operate on the hardware layer („below“ OS)
- Virtually all common CPUs are affected by at least one of both

Attack	Intel	AMD	ARM *	IBM Power
Meltdown	✓			
Spectre	✓	✓	✓	✓

* ARM CPUs are mostly used in smartphones and tablets, including Apple's CPUs

- Researchers named the vulnerabilities „worst of all times“ because of the huge number of affected devices and the independence from employed operating systems

Meltdown & Spectre – Worst Computer Vulnerabilities Ever

- Both attack scenarios allow attackers to read from memory, that should not be accessible from the process which they can control
 - attackers can read secrets, e.g., passwords or cryptographic keys residing in memory, even via JavaScript in the browser
 - browser vendors came up with own patches very early
- Disastrous for cloud companies, where computing resources of different customers are running on the same physical hardware
 - attacker just needs to rent a Virtual Machine and is able to spy out other customers' data
 - cloud companies were the first to report that patches have been applied

Recently Detected CPU Vulnerabilities: Meltdown in Detail (1/4)

- Programs often take decisions how to proceed during the execution, what leads to “execution branches”
- To increase performance, CPU pre-executes branches of program code in advance, e.g., when it has to wait for read/write operations
 - if a branch becomes relevant later, CPU already did the work – “**speculative execution**”
 - for such “**speculative execution**” no security checks are applied
 - later, if a pre-executed branch is really chosen, a security check is performed and prevents unauthorized access to memory

Recently Detected CPU Vulnerabilities: Meltdown in Detail (2/4)

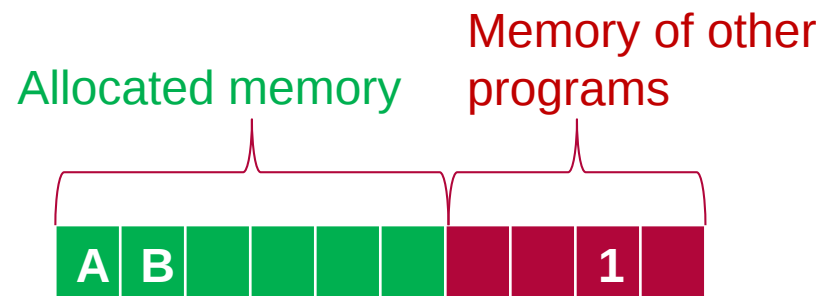
- CPU cache is faster than “regular” memory
 - usually, after a first access to the needed data, it gets stored in a CPU cache
 - by measuring access time, attacker can determine if data was read from CPU cache or memory

Recently Detected CPU Vulnerabilities:

Meltdown in Detail (3/4)

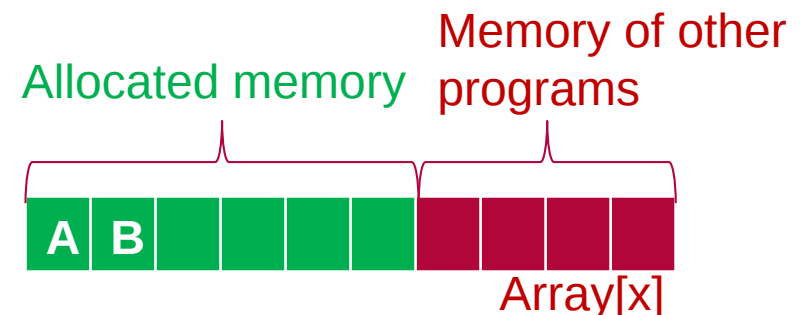
- Attacker writes code in a branch that reads the memory outside of the allowed area (memory of other program)
- Branch will be pre-executed speculatively before CPU knows that it accesses memory outside of the allowed part (no security check)
 - that branch of code can read the value, e.g., **1** or **0**
- Next, attacker reads some other data (from memory he/she is allowed to access) into the CPU cache, depending on the value from accessed memory (still in the pre-executed branch):
- ```
if read_value == 1
 load A into cache
else if read_value == 0
 load B into cache
end
```

  - here: **A** is loaded



# Recently Detected CPU Vulnerabilities: Meltdown in Detail (4/4)

- Then security checks will be applied, the pre-executed branch will be reverted and the value from accessed memory, as well as **A** and **B** will **not** be returned
  - however, the CPU cache will not be cleared, **A** is still in the cache!
- Next, attacker re-reads **A** and **B** from memory
  - If access to one is faster than to the other attacker knows that it was cached from speculative execution
    - Here: **A** is read faster than **B** (**A** cached, **B** not)
    - **Attacker knows: accessed memory was 1 and not 0**
- Attacker can repeat this procedure and read larger amounts of data from memory that actually belongs to other programs



# Patches for Meltdown and Spectre

---

- Luckily, software update can fix both Meltdown and Spectre
  - On the CPU level:
    - Intel released a CPU firmware update, but it causes reboot issues (as of January 24th)
  - On the OS level:
    - Linux, Windows and OS X released patches already
  - On the application level:
    - Browsers (Firefox, Edge, and Chrome) have released their own OS-independent patches
- However: software patches may result in performance loss (e.g. 2-7% on Intel CPUs)
  - Hardware vendors must implement new concepts in future CPUs to overcome this
- **Keeping your system up-to-date is extremely important!**