# SEED SECURITY LABS

# Spectre Attack Lab

## General problem

- Modern microprocessors[1] perform branch prediction and speculative execution of instructions.
- So, they achieve (apparent) high execution speed when the prediction is true (what should happen a significant number of times).
- When prediction is wrong, the state of the processor is returned to the correct state, corresponding to the correct branch being taken;
  - unfortunately, some of the wrong leftovers are not deleted: processor cache is the common example (durable side effect).
- A subsequent probing of cache, may reveal secretive data!

[1] Intel, AMD, ARM...

## ...General problem

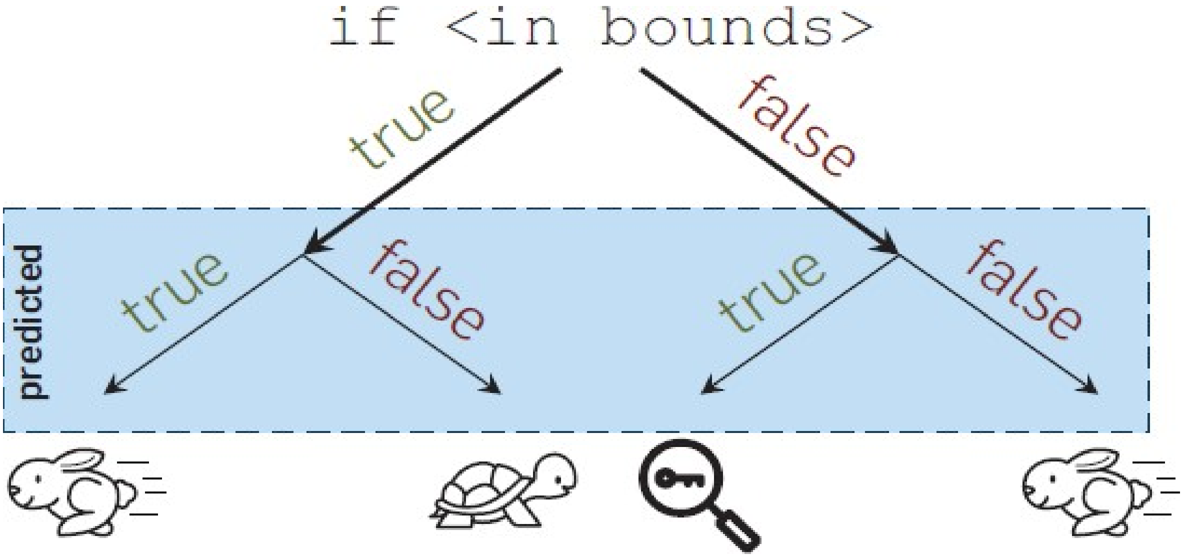

*Figure 1. Before the correct outcome of the bounds check is known, the branch predictor continues with the most likely branch target, leading to an overall execution speed-up if the outcome was correctly predicted. However, if the bounds check is incorrectly predicted as true, an attacker can leak secret information in certain scenarios. (in "Spectre Attacks: Exploiting Speculative Execution")*

# Spectre attack procedure

- setting up
  - mistrain processor prediction logic
  - flush relevant data from cache
- forcing prediction failure
  - with knowledge of secretive code & data, force speculative execution
  - as a result, cache will retain secretive data (although correct data will be provided in processor registers and memory)
- collecting secretive data by side-channels
  - typically, by timing the reading access to cache lines, secretive data is revealed, as is accessed faster
- *Important*: with Spectre[1] one does not want to trigger traps or exception handling of kernel

[1] contrary to Meltdown attack

# Hardware bug

- CVE-2017-5715 / CVE-2017-5753
  - *«Systems with microprocessors utilizing speculative execution and indirect / direct branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.»*
- Spectre Attacks: Exploiting Speculative Execution[1]
  - «(...) *Spectre attacks involve inducing a victim to speculatively perform operations that would not occur during correct program execution and which leak the victim's confidential information via a side channel to the adversary*. (...)»
  - «(...) *These attacks represent a serious threat to actual systems since vulnerable speculative execution capabilities are found in microprocessors from Intel, AMD, and ARM that are used in billions of devices*. (...)»

[1] original paper includes Spectre example implementation!