Secure Programming Answer 1

1 RIDL and Fallout

1.1

Security researchers consider RIDL and Fallout inspired by previous speculative execution attacks, including Meltdown and Spectre. Study the CVE entries and related documentations for RIDL and Fallout, in your own words briefly describe what is a speculative execution attack and the similarities and differences of RIDL and Fallout comparing to Meltdown and Spectre.

Answers:

Speculative execution is wildly used in modern CPU. Most modern CPUs will assume the next operation and pre-execute that code fragment if extra resources are available. These pre-executed results will be saved in cache instead of committing directly, further estimation will identify whether they will be used or abandoned. For instance, the code after raising exception should not be executed, but in speculative execution it will, and the results will be saved in cache, when committing all the results, CPU find that there is an exception so the result of successive code will be discarded.

A speculative execution attack exploits this feature to leak data from privileged parts. As only the data from speculative execution will be saved in cache and we all know that picking data from cache is significantly faster, so when the attack access to all the entries, which entry that executing time much less than the others contains the leaked information.

Similarities

* All RIDL, Fallout, Meltdown and Spectre are based on speculative execution to allow unprivileged users to leak data from privileged parts.
* They all exploit side channels to leak data.
* They all exploit some microarchitectural (hardware) implementation issues rather than software implementation issues.

Differences

* Meltdown and Spectre generally leak data from cache while RIDL and Fallout can exploit side channels even in 4 latest released Microarchitectural Data Sampling (MDS).
* RIDL and Fallout can even attack the privileged parts without speculative executions, which means these two attacks can run speculative execution from error-free and branchless unprivileged execution.

1.2

There are four CVE entries describing RIDL and Fallout, please identify which of them is (are) describing RIDL and which of them is (are) describing Fallout.

RIDL:

CVE-2018-12127 (Microarchitecture Load Port Data Sampling)

CVE-2018-12130 (Microarchitecture Fill Buffer Data Sampling)

CVE-2019-11091 (Microarchitecture Data Sampling Uncacheable Memory)

Fallout:

CVE-2018-12126 (Microarchitecture Store Buffer Data Sampling)

1.3

Identify the Common Weakness (using CWEs) for these two vulnerabilities. Also identify which scope in the CIA triad has been violated by the common weakness and why.

I think the **confidentiality** principle has been violated because the vulnerabilities allow the unprivileged users to gain the ability to obtain the protected data. So that the **integrity** cannot be guaranteed as well because during the time the data saved in cache, the unprivileged users can operate on those data as well.

1.4

Identify the possible consequences of these vulnerabilities and how an attacker can make use of the consequences.

Consequences:

* the sensitive information / data make be leaked like account name and password.
* do injection, attacker may insert, remove or change some data after obtaining it.

usage:

* attacker can become authenticated user after getting account information
* Data integrity can be broken, modify data or add commands so that for example, to break data base (remove existed records; add invalid / useless records; steal the records away), change the calculate result or even crash the program or computer.

1.5

These two vulnerabilities are considered to be “hardware” vulnerabilities. Briefly discuss the difference between hardware vulnerabilities and software vulnerabilities and how you might draw a distinction. To help your explanation, give an example of one software vulnerability and one other hardware vulnerability that are listed in the NVD (https://nvd.nist.gov) and occurred in the last two years.

Remark: No marks will be given if you give an example of RIDL/Fallout/Meldown/Spectre.

In my opinion, hardware vulnerabilities can be seen as weaknesses that allow attackers to gain physical access to hardware; or flaws in system design that allow attackers to boost their privileges to maliciously leak data or execute their own codes.

And software vulnerabilities can always be unexpected weaknesses or bugs during designing the architecture of software or implementing actual code.

1.6

“RIDL and Fallout are so dangerous. After I heard about these vulnerabilities, I did a full scan of my computer by the latest anti-virus software and installed all application updates. The anti-virus protection does not find any problems. I have also installed a personal firewall in my computer. So I strongly believe that my computer should be secure enough to defend RIDL and Fallout attacks.”

-By Mr. Super Secure

State your opinion and discuss whether you agree or disagree with Mr. Super Secure’s words. Provide some reasons to support your opinion, explaining the role of PC security software mentioned.

1.7

Apart from installing the above mentioned security software, please describe two possible measures to protect your computer from RIDL and Fallout attacks.