Indian Institute of Technology Bombay

CS305/341

Computer Architecture

i7: Spectre and More

Authors:	*Roll Number:*
Sanchit Jain	160050043
Charith	160050083
Rahul	160050072
Suraj	1600500XX
Jeevitesh	1600500XX

November 6, 2018

Contents

1 Abstract **2**
1.1 What is it About? . . . 2
1.2 Can someone Explain in Simple words? . . . 2

2 Baby Steps/Background **3**
2.1 Out of order Execution . . . 3
2.2 Speculation Execution . . . 3
2.3 Branch Prediction . . . 3
2.4 The Memory Hierarchy . . . 3
2.5 Microarchitectural Side-Channel Attacks/Flush-Reload Techniques . . . 3
2.6 Return Oriented Programming . . . 3

3 What is Spectre? Why is it more famous than me? **3**
3.1 General . . . 3
3.2 Varient1 . . . 3
3.3 Varient2 . . . 3
3.4 Varient4 . . . 3

4 Our Result(Code+Result(screenshot)) **3**

5 Proof of Concept Study **3**

6 The Experiment **3**
6.1 Our Result . . . 3
6.2 Our Technique . . . 3

7 Mitigations **3**
7.1 Preventing Speculative Execution . . . 3
7.2 Preventing Access to Secret Data . . . 3
7.3 Preventing Data from Entering Covert Channels . . . 3
7.4 Limiting Data Extraction from Covert Channels . . . 3
7.5 Preventing Branch Poisoning . . . 3

8 Current Work Going On **3**

9 Conclusion **3**

10 Acknowledgement **3**

1 Abstract

1.1 What is it About?

This is a simple report template with the UCT logo. Feel free to use/modify it to suit your needs. Variables that need to be altered have been commented to make modifications easier. For example if you need to change the university logo, look for the comment `% University Logo` in this file and then make appropriate modifications in that line.

A Table of Contents and a bibliography have also been implemented. To add entries to your bibliography, simply edit `biblist.bib` in the root folder and then use the `\cite{...}` command in `main.tex` [1]. The Table of Contents will be updated automatically.

I hope that you find this template both visually appealing and useful.

1.2 Can someone Explain in Simple words?

— Linus

2 Baby Steps/Background

2.1 Out of order Execution

2.2 Speculation Execution

2.3 Branch Prediction

2.4 The Memory Hierarchy

2.5 Microarchitectural Side-Channel Attacks/Flush-Reload Techniques

2.6 Return Oriented Programming

3 What is Spectre? Why is it more famous than me?

3.1 General

3.2 Varient1

3.3 Varient2

3.4 Varient4

4 Our Result(Code+Result(screenshot))

5 Proof of Concept Study

6 The Experiment

6.1 Our Result

6.2 Our Technique

7 Mitigations

7.1 Preventing Speculative Execution

7.2 Preventing Access to Secret Data

7.3 Preventing Data from Entering Covert Channels

7.4 Limiting Data Extraction from Covert Channels

7.5 Preventing Branch Poisoning

8 Current Work Going On

9 Conclusion

10 Acknowledgement

References

[1] Help on BibTeX entry types. http://nwalsh.com/tex/texhelp/bibtx-7.html. Accessed: 2015-03-12.