



INDIAN INSTITUTE OF TECHNOLOGY BOMBAY

CS305/341

COMPUTER ARCHITECTURE

---

## i7: Spectre and More

---

*Authors:*

Sanchit Jain

Charith

Rahul

Suraj

Jeevitesh

*Roll Number:*

160050043

160050083

160050072

1600500XX

1600500XX

November 6, 2018

## Contents

<b>1</b>	<b>Abstract</b>	<b>3</b>
1.1	What is Spectre? . . . . .	3
1.2	Can someone Explain in Simple words? . . . . .	3
1.3	Is is Really a ghost? . . . . .	3
<b>2</b>	<b>Baby Steps/Background</b>	<b>4</b>
2.1	Out of order Execution . . . . .	4
2.2	Speculation Execution . . . . .	4
2.3	Branch Prediction . . . . .	4
2.4	The Memory Hierarchy . . . . .	4
2.5	Microarchitectural Side-Channel Attacks/Flush-Reload Techniques . .	4
2.6	Return Oriented Programming . . . . .	4
<b>3</b>	<b>What is Spectre? Why is it more famous than me?</b>	<b>4</b>
3.1	General . . . . .	4
3.2	Varient1 . . . . .	4
3.3	Varient2 . . . . .	4
3.4	Varient4 . . . . .	4
<b>4</b>	<b>Proof of Concept Study</b>	<b>4</b>
<b>5</b>	<b>The Experiment</b>	<b>4</b>
5.1	Our Result . . . . .	4
5.2	Our Technique . . . . .	4
<b>6</b>	<b>Mitigations</b>	<b>5</b>
6.1	Preventing Speculative Execution . . . . .	5
6.2	Preventing Access to Secret Data . . . . .	5
6.3	Preventing Data from Entering Covert Channels . . . . .	5
6.4	Limiting Data Extraction from Covert Channels . . . . .	5
6.5	Preventing Branch Poisoning . . . . .	5
<b>7</b>	<b>Current Work Going On</b>	<b>5</b>
<b>8</b>	<b>Conclusion</b>	<b>5</b>
<b>9</b>	<b>Acknowledgement</b>	<b>5</b>
	<b>Appendices</b>	<b>7</b>

<b>A : Meltdown. Lets melt its cocoon</b>	<b>7</b>
<b>B : Onomastics of Spectre and Meltdown</b>	<b>7</b>

# **1 Abstract**

## **1.1 What is Spectre?**

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?**

## **1.3 Is is Really a ghost?**

**Yes!**

## **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 Variet1**

### **3.3 Variet2**

### **3.4 Variet4**

## **4 Proof of Concept Study**

## **5 The Experiment**

### **5.1 Our Result**

### **5.2 Our Technique**

## **6 Mitigations**

### **6.1 Preventing Speculative Execution**

### **6.2 Preventing Access to Secret Data**

### **6.3 Preventing Data from Entering Covert Channels**

### **6.4 Limiting Data Extraction from Covert Channels**

### **6.5 Preventing Branch Poisoning**

## **7 Current Work Going On**

## **8 Conclusion**

## **9 Acknowledgement**

## References

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

# Appendices

## A : Meltdown. Lets melt its cocoon

**PersonX:** Do you have a Sibling?

**Spectre:** Ahh yes I have one named Meltdown

**PersonX:** Can you tell us something about it?

**Spectre:** Like every pair of Siblings we are from same Parents. The basic ideologies and mechanism through which we arise are the same. We both are based on Speculative Execution/Branch Prediction. But yet we are not the same. It is different from me in the following sense.

## B : Onomastics of Spectre and Meltdown

**PersonX:** What was the reason that your parents chose these names for you?

**Spectre:** Well I don't know. You should go and ask my parents I suppose. From what they have told me or what many believe is the following reason. For me it is because since my internals are based on '**Speculative Execution**' so they wanted something similar sounding.

When I was born/discovered they knew I am very dangerous to a department called cyber security hence one of my parents **Paul Kocher** named me "Spectre" which really means a **ghost**. I not only was supposed to **haunt the cyber security professionals** but also was largely **invisible** to the ordinary program execution.

**PersonX:** What about the naming of "Meltdown"?

**Spectre:** The thinking of the name of "Meltdown" actually ironically haunts me and makes me really jealous. It is believed to be coined by one of my parent **Daniel Gruss** . The reason given for this coining of name was that since it **melts the boundary between programs** and **OS** it is aptly called "Meltdown". The name



also made it sounds really devastating, with a huge impact, like an actual **meltdown in a nuclear reactor**.

Moreover, in **German**, meltdown is '**Kernschmelze**', which means '**melting of the core**'. Since we call the CPU as a core and indeed a 'CPU Kern' so it is also a wordplay, implying that the CPU is not in a good condition."