

Programming Assignment 1
(Cache Covert and Side Channel Attack)
CS665: Secure Memory Systems
2019-20 - Semester I
Computer Science and Engineering Department
Indian Institute of Technology Kanpur
Due Date: 12th September 2019, 11:55pm

August 11, 2019

This programming assignment is designed to ensure that you are acquainted with the working principle of CPU Cache and its related security issues. In this assignment, you need to create a Cache Covert Channel to share information between Gogo and Gollu, running on two cores, in a multi-core system. Prior to create your covert channel, you can go through the “**FLUSH+RELOAD**” attack to get a feel and how to kick-start. The details about the attack is available in the web-link <https://github.com/Anish-Saxena/Flush-Reload>. Once you understand the whats, hows, and whys, you are ready to go. You can download/clone the code base and all other relevant files for PA1 from the following link <https://git.cse.iitk.ac.in/skmtr/CS665-2019-PA1>

Part 1: Cache Covert Channel (FLUSH+RELOAD)

This part of the assignment deals with creating a covert channel between Gogo and Gollu that are running on two separate physical cores. They cannot communicate directly for confidentiality reasons and that's why they need to create a covert channel to communicate so that no other processes could get the information. **This part consist of two tasks:**

Task 1a [It is Damn Easy !! 5 Points]: In this **task**, you need to create a **Cache Covert Channel** using **FLUSH+RELOAD** where **Gogo** reads some information from the terminal and sends it to the **Gollu**. You can assume that the information read from the terminal will not be of more than 50 characters. You have to report the covert channel bandwidth and the accuracy of the channel.

Task 1b [This is the real assignment !! 10 Points]: This Task is an extension to **Task 1a**. You need to share secret information but this time it will be a **text** file. You can choose any **text** file :). This task is further divided into the following subtasks:

1. **Gogo** first reads a filename from the terminal and communicate the filename to **Gollu** using the covert channel. You can assume that the file to be send will be in the current working directory of **Gogo**.
2. After receiving the file name, **Gollu** creates a new blank file by appending **received_** in front of the filename received from **Gogo**.

3. After sending the filename, **Gogo** then read the content of the file and communicate it to **Gollu** using covert channel again!
4. **Gollu** then writes all the received contents into a file that is earlier created by **Gollu**.
5. You have to report the covert channel bandwidth and the accuracy of the channel.

[Note: Gogo and Gollu's current working directories are different]

Cache Side Channel on GnuPG

Task 2a [easy peasy lemon squeezy, 5 Points]: In this task, you need to perform the **FLUSH+RELOAD** attack on **GnuPG** cryptography Library to observe accesses to critical functions like **Square (S)**, **Module (r)**, and **Multiply (M)** function during the encryption or decryption process of the RSA algorithm. For this assignment, **Gogo** will mount a side-channel attack with a goal to leak the critical accesses of **Gollu**. You have to report True Positive Rate and False Positive Rate of the side-channel.

If you want the Bonus points

Task 3a [Sounds interesting: Gogo and Gollu as Romeo and Juliet, 5 Points]: In this task, **Gogo** sends his heart (soul may be, in the form of an **image** file) to **Gollu** over the **Cache Covert Channel**, created using **FLUSH+RELOAD** attack. You have to report the covert channel bandwidth and the accuracy of the channel.

[Note: All the information sharing has to be performed through the Cache covert channel only. All the task(s) has to be done on Linux Operating System. We will accept your submission via Canvas only, and any other submission mode is strictly prohibited such as submitting via email or piazza. While using Piazza/email for discussions, use CS665-PA1 as the header]

Deliverable:

1. Source code for **Task 1a**, **Task 1b**, and **Task 2a** along with the **Challenge task** if attempted. Document your code properly. Share your results (wait for Biswa's lectures) and experiences in a pdf: Why something worked/not worked, any insights, any experiments that you did to validate your assumptions/confusions. Biswa will talk about it in details.
2. In the pdf, Also provide division of labor: Who did what, Say Biswa did Task 1a, Biswa2 did Task 1b and 25% of Task 2a.
3. Feel free to discuss about the assignment among your friends and with Biswa, Saurabh, Sujeet and Upasana. However, at the end of the day, we want you to do everything on your own.
4. Write a **README** file including what you have discussed with whom and any other sources that you have referred to for the assignment. If you have used any scripts/code from your friends, do mention that as well.

All the best. Looking forward to the submissions !!

PS: Start Early.