1 Master's Thesis

My Master's thesis was my first research experience. I was advised by Professors Giorgio Buttazzo and Tommaso Cucinotta at Scuola Superiore Sant'Anna, and co-advised by Björn Brandenburg, head of the Real-Time Systems group at the Max Planck Institute of Software Systems, where I spent seven months. My project was about increasing the predictability of real-time tasks in multi-core systems by implementing a cache-partitioning technique, called 'page coloring', in the latest Linux kernel.

With page coloring, tasks running on different cores are assigned different cache partitions ('colors'), preventing them from interfering with each other. This guarantees *a priori* that the tasks on the system meet their timing constraints - that is, the system is predictable. In order to implement page coloring at the operating system level, it is necessary to modify the physical memory page allocation mechanism such that tasks are allocated pages that are mapped to different cache partitions.

The project had three big challenges. First, the documentation for the Linux memory management module was outdated and insufficient. Therefore, I conducted a preliminary study of the memory allocators by running a function tracer in the kernel. With the results obtained from the tracer, I could gain a deeper understanding on how to design my solution.

Second, the debugging tools that are typically available for the Linux kernel fail if the underlying memory allocation mechanism does not meet their assumptions. In my project, I had to modify the core structure of low-level memory allocators, rendering most debuggers unusable: this includes useful tools to detect whether a process is accessing a memory location after freeing it, or if a process is using an address that belongs to another process. Without being able to benefit from the standard kernel development tools, I had to create my own debugging framework.

Third, I could not implement the page coloring mechanism directly on the physical page allocator because page coloring requires processes to request pages that are not contiguous in physical memory. As there is no central point in which the physical-to-virtual address mapping takes place in the page allocator, I had to modify the translation mechanism of two additional, higher-level, kernel memory allocators.

At the end of my research visit at the Max Planck Institute, I had enough material to graduate, but my project was not complete. Therefore, I decided to continue working on my thesis with my advisors at Scuola Superiore Sant'Anna for three additional months, until I obtained a working implementation. During this time, I had the opportunity to collaborate with experienced researchers and engineers who assisted me in finding a solution to my challenging project. Even though my

implementation was still affected by minor bugs, I could conduct experiments to show the effectiveness of my work. With my solution, the effect of interference on task execution times was reduced from 14.6% to 4.4%. The remaining interference is likely attributed to shared components other than the cache, which affect task execution times nondeterministically.

2 Research Visit at Northeastern University

Currently, I am a visiting researcher at Northeastern University, advised by Professor Alan Mislove. My project is about the implications of targeted advertising on users' privacy.

Social networks collect and store a large amount of information about people. Additionally, their ad platforms provide advertisers with a number of tools to target users directly. For instance, the Custom Audience feature on Facebook Ads lets advertisers upload a list of users to whom they want to show their ads. If not carefully implemented, these tools can leak users' personal information to advertisers.

I am reverse-engineering the targeted advertising features of the Facebook Ads platform to show how an adversary can exploit the interface to infer other users' personal information and online activity. The attacks I am designing cannot be detected by the victim and do not require the adversary to interact with the victim.

My current task is to reverse-engineer the size estimates provided by the Facebook Ads platform for targeted advertising audiences. This is challenging and it requires a set of principled experiments to pinpoint the particular obfuscation mechanism being used by Facebook.

Another challenge I am facing is that of proposing a fix to provide a robust defense to the attacks, while preserving the main functionalities that make the Custom Audience feature appealing to advertisers.

My work will be submitted to a major security conference at the beginning of next year.