April 17

Tuesday

Colloquium

Faculty of Computer Science, HSE

Guilhem Gamard

HSE

The Meltdown Attack

Modern CPU hardware implement a memory-protection mechanism to prevent one process from reading memory of another process. A few months ago, several vulnerabilities in this mechanism were published; this talk explains one of them, called Meltdown. This attack allows one process to read the whole memory of the machine on which it currently runs. This mostly concerns cloud-computing providers, as virtual machines running on the same physical server can spy each other.

Meltdown received vast coverage because it impacts virtually any Intel CPU currently on the market, and because it has existed for about 20 years before it was discovered. Operating systems vendors have implemented, in software, techniques to mitigate Meltdown; they claim that those security patches induce performance loss in running applications.

In this talk, we will review some features of modern CPUs, then we will explain how to exploit them to bypass memory protection. Finally, we will see how operating systems were modified to mitigate this risk.

April 17, 18.10–19.30
Kochnovskii proezd, 3, room 205

Register at https://cs.hse.ru/en/colloquium